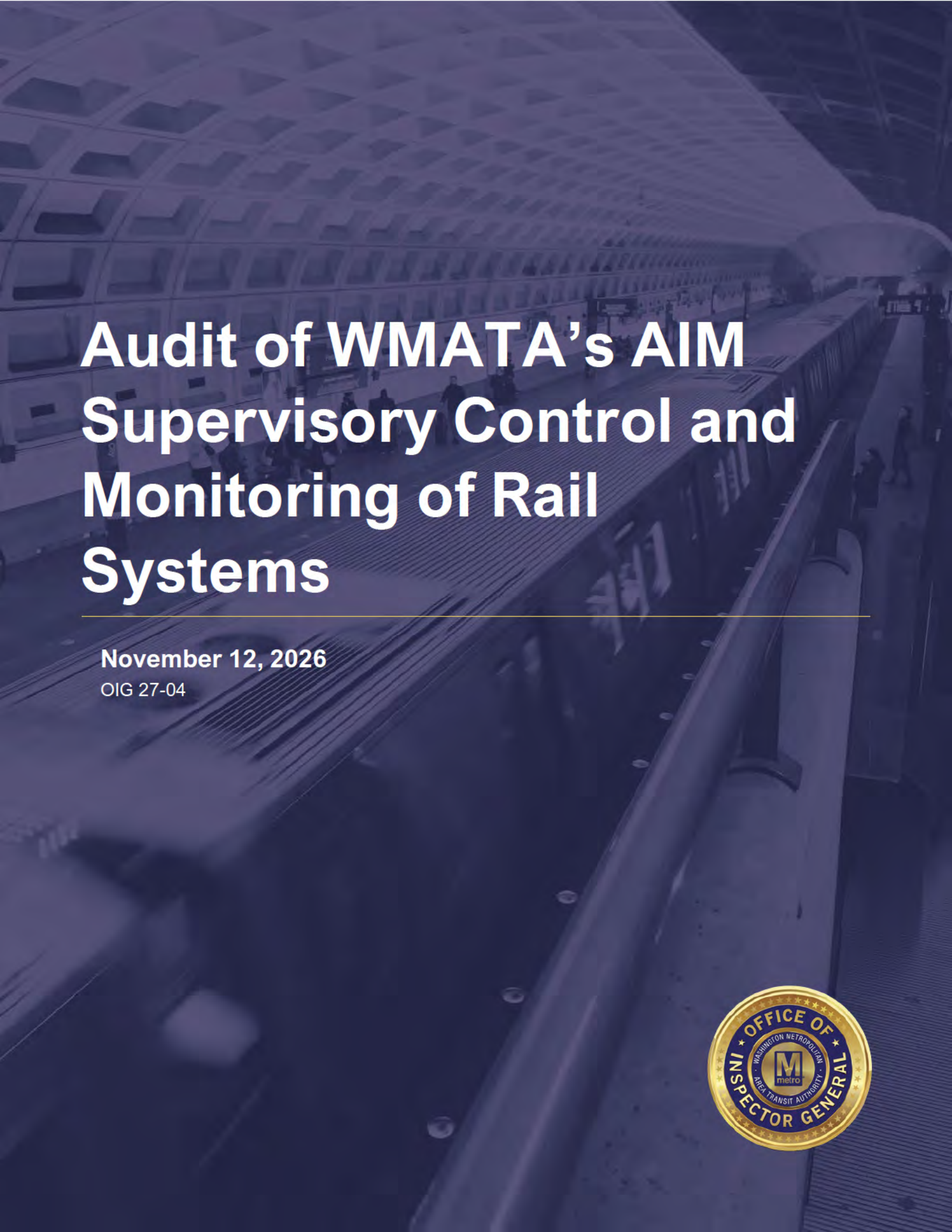


Audit of WMATA's AIM Supervisory Control and Monitoring of Rail Systems

November 12, 2026

OIG 27-04

Results in Brief

Audit of WMATA's AIM Supervisory Control and Monitoring of Rails Systems

Audit Objective

The audit objective was to determine whether the Washington Metropolitan Area Transit Authority (WMATA) has implemented effective governance to ensure the Advanced Information Management (AIM) system provides safe, reliable, resilient, scalable, and cost-effective supervisory monitoring and control of critical train operations.

Why We Did the Audit

- WMATA is modernizing its rail system by replacing Remote Terminal Units (RTUs), upgrading to fiber optic media, and implementing a Communications-Based Train Control (CBTC) system. Evaluating the reliability, governance, cybersecurity, resiliency, and modernization readiness of the AIM infrastructure is critical to supporting safe, reliable, and resilient rail operations.

- This audit was included in the Office of Inspector General's (OIG's) Fiscal Year (FY) 2026 Annual Audit and Evaluation Plan.

- The Infrastructure Investment and Jobs Act requires OIG to assess how effectively WMATA is using funding for capital improvement projects. The AIM system falls within this required assessment.

Recommendations

OIG identified 33 recommendations to help WMATA modernize its supervisory control and monitoring system.

What OIG Found

OIG found significant deficiencies with the AIM system. Specifically, OIG found:

1. DM has not established a continuity strategy for the legacy AIM system
2. DM has not effectively managed vendor and key-person dependencies or ensured adequate contract oversight
3. WMATA relies on outdated RTUs and legacy communication infrastructure
4. WMATA does not effectively manage critical AIM configuration settings
5. WMATA lacks effective AIM operational data governance and management
6. WMATA lacks effective AIM alarm management, root cause analysis, and system performance monitoring
7. Physical access controls to critical train control rooms need strengthening
8. Cybersecurity controls over AIM and interfaced train control systems need strengthening
9. WMATA lacks integrated risk management over the AIM system
10. Red line CBTC migration readiness is limited by AIM technical deficiencies and the lack of a vendor-neutral CBTC reference and integration architecture







Table of Contents

Background 4
Finding 1 7
Recommendations 1-3 9
Finding 2 13
Recommendations 4-6 15
Finding 3 18
Recommendations 7-9 23
Finding 4 26
Recommendations 10-12 30
Finding 5 33
Recommendations 13-14 35
Finding 6 37
Recommendations 15-19 40
Finding 7 45
Recommendation 20 46
Finding 8 48
Recommendations 21-25 51
Finding 9 55
Recommendations 26-30 58
Finding 10 63
Recommendations 31-33 66

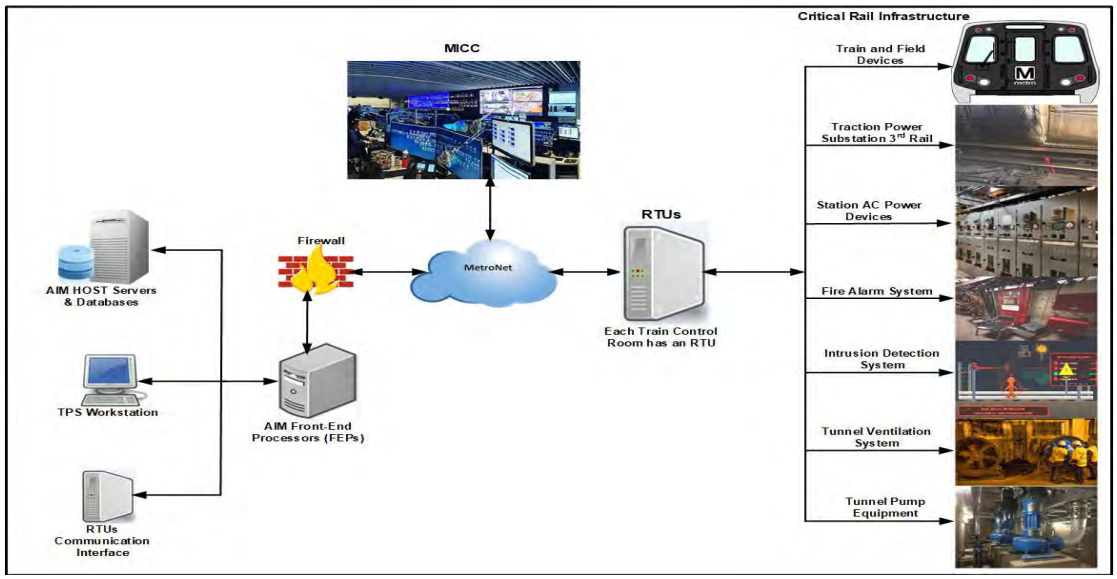
Appendix 69
Appendix A: Scope & Methodology 69
Appendix B: Glossary 71
Appendix C: AIM Deficiencies Affecting CBTC Implementation 74
Appendix D: Summary of Management's Response 75
Appendix E: Management's Response 76

The Advanced Information Management (AIM) system is a proprietary, mission-critical rail operations Supervisory Control and Data Acquisition (SCADA) platform that the Washington Metropolitan Area Transit Authority (WMATA) implemented in April 1998. It provides WMATA real-time monitoring and control of train movement, interlockings, traction and station power, intrusion detection, and tunnel equipment, including ventilation, pumps, and auxiliary systems.

Overview of the AIM System

Remote Terminal Units (RTUs), microprocessor-based field devices located at each station that collect and transmit data from operationally critical wayside devices, send real-time data to the AIM system for processing and make the information available for WMATA's Metro Integrated Command and Communications Center (MICC).[1] Dispatchers and supervisors at the MICC use that data to monitor conditions, respond to alarms, coordinate maintenance, and support service recovery (*see* **Figure 1**). In addition, AIM interfaces with key systems such as Rail Performance Monitoring (RPM), Train Progress Server (TPS), and the Passenger Information Display System (PIDS) to deliver real-time information that supports safe, reliable, and efficient rail operations and passenger information.

Figure 1: WMATA Conceptual AIM System Architecture



[1] *The MICC is WMATA's primary operations center, integrating bus, rail, infrastructure, safety, and power functions.*

In the event of an AIM failure or outage, WMATA has established contingency procedures to manually maintain rail service. Under those procedures, the Automatic Train Control (ATC) Maintenance Team dispatches personnel to the field to ensure safe train separation and speed enforcement conditions are met. Although these procedures allow trains to continue operating safely, they do not replace AIM's real-time supervisory capabilities.

WMATA's Rail Modernization Program

WMATA's Board of Directors approved a $913 million, multi-year Red Line Modernization Program as part of its FY 2027 Budget Strategic Transformation Plan. The program will replace the current ATC system with a Communications-Based Train Control (CBTC) system for the Red Line.[2] As WMATA moves to CBTC, it will continue to rely on the AIM, or a future successor supervisory control platform, to support safe and reliable rail operations. Accordingly, the condition, reliability, and modernization readiness of AIM are important considerations for successful CBTC implementation and long-term rail operations.

Departmental Responsibilities for AIM

AIM operations depend on coordination across the following departments, each responsible for managing different components:

- ***Digital Modernization (DM***) - maintains and supports the AIM system through its Operations Technology (OT) team, in coordination with the vendor [redacted]

- ***Communications and Signaling (COSI***) - oversees the planning, design, and maintenance of Metro's safety-critical infrastructure, including RTUs, train signaling, radio systems, fire alarms, and passenger information displays.

- ***Power Engineering (Power)*** - maintains WMATA's SCADA systems, including AIM, which supports traction power and tie breaker systems, auxiliary power for stations and facilities, electric buses, and other critical systems.

[2] *The FTA and Institute of Electrical and Electronics Engineers define CBTC as an advanced signaling system that uses continuous two-way communications between trains and wayside equipment to determine precise train location and automatically maintain safe separation, improving safety, capacity, and overall rail operating efficiency.*

- ***The MICC*** - uses AIM to monitor and control train movements, traction power, and station equipment through real-time data displayed on control room systems and projection screens.

Funding Sources for Upgrades to AIM and RTUs/Train Control Rooms (TCRs)

In November 2021, Congress and the President enacted the Infrastructure Investment and Jobs Act (IIJA). The act requires the OIG to issue reports two years and five years after the enactment of the IIJA that include, among other things, an assessment of the effective use of funding to address major Capital Improvement Program (CIP) projects. As part of this effort, OIG identified several CIP initiatives potentially related to AIM that fall within the scope of this assessment. These programs will be incorporated into the five-year IIJA report.

Finding 1: WMATA Has Not Established a Continuity Strategy for the Legacy AIM System

WMATA has not established a long-term strategy for the AIM system, nor has it implemented adequate continuity protections. These include establishing contractual rights to software, performing periodic evaluations of system performance, and assessing system integration capabilities – protections necessary to ensure continued operation of the AIM system in the event of a major failure or transition to a new platform. Without these safeguards, WMATA lacks reliable assurance that AIM can continue supporting supervisory control of critical rail operations.

Specifically, OIG made the following observations:

a. **AIM Software Escrow or Source Code Access Protections**: The AIM system is proprietary software owned and maintained by the vendor. However, WMATA has not established a software escrow agreement or contractual rights to obtain the AIM source code and other critical software assets if the vendor becomes insolvent, ceases operations, discontinues support, or is otherwise unable to fulfill its contractual obligations.

   According to the Control Objectives for Information and Related Technology[3] (COBIT) 2019 guidance,[4] organizations should implement software continuity arrangements to help ensure critical systems remain available and recoverable during service disruptions. These practices include software escrow, contractual source code access, and documented software recovery procedures.

   Without these safeguards, WMATA has limited assurance that it can independently restore, maintain, or modify the AIM system following a vendor failure or other disruption. This increases the risk of prolonged service disruptions, reduced operational resilience, higher lifecycle costs, delayed system recovery, and continued dependence on a single vendor to support a mission-critical rail system.

---

[3] *COBIT is a globally accepted framework for optimizing enterprise information technology governance.*

[4] *COBIT. 2019 Framework: Governance and Management Objectives - DSS04.02, Business Resilience; DSS04.03, Continuity Response; and DSS04.07, Backup Arrangements.*

b. Technical Solution Assessments: As AIM continues to age and operational needs change, WMATA should periodically evaluate system performance, lifecycle, and available technology options. These technical solution assessments help ensure critical systems remain reliable, supportable, maintained in a State of Good Repair (SOGR), and capable of meeting future operational and modernization needs. However, WMATA has yet to perform a technical solution assessment to determine whether AIM remains the most appropriate long-term supervisory control platform.

The Federal Transit Administration (FTA) Transit Asset Management (TAM) Rule (49 CFR Part 625) requires transit agencies to manage critical assets throughout their lifecycle, maintain them in a SOGR, and make risk-informed investment decisions that support safe and reliable transit operations.[5] Also, in line with best practices, the National Institute of Standards and Technology (NIST) guidance further recommends periodically evaluating the performance, reliability, maintainability, interoperability, and lifecycle suitability of operationally critical control systems to support informed technology decisions and long-term operational resilience.[6] These standards require, or recommend, that WMATA determine whether the AIM system can meet current and future operational requirements.

By not conducting technical solution assessments, WMATA has limited insight into whether the AIM system meets current and future operational needs. The absence of benchmarking and industry or vendor comparisons increases the risk of reduced reliability, higher lifecycle costs, and constrained scalability.

c. System Integration Assessment: WMATA has not conducted a system integration assessment for the AIM system. An integration assessment confirms the compatibility of the AIM system with other interconnected systems and devices.

For instance, WMATA's lack of an integration assessment led to integration issues during the implementation of the Tagging Relay, a safety control function that automates the remote de-energization and re-energization of the third rail from the MICC. The Tagging Relay uses Distributed Network Protocol, version 3 (DNP3) for communication.[7] However, it could not function properly because the AIM system

[5] *FTA. 49 CFR Part 625: Transit Asset Management, §§ 625.5, 625.17, 625.25, 625.33, and 625.41. 2026.*

[6] *NIST. Special Publication 800-82, Revision 3. Guide to Operational Technology OT Security. September 2023.*

[7] *DNP3 is a set of communication protocols used between components in process automation systems, such as RTU systems.*

was not fully compatible with DNP3. Thus, the MICC's ability to remotely control third rail de-energization and re-energization was degraded. WMATA may have detected these integration issues earlier had it conducted an integration assessment.
Federal guidance emphasizes the importance of these evaluations. The FTA's Project and Construction Management Guidelines state that transit system elements should be planned and engineered with appropriate interfaces and that system integration activities should confirm that system elements are mutually compatible and function together as an integrated system.[8] Similarly, NIST Special Publication 1108, Revision 4, recognizes that differences in communications protocols can affect interoperability among interconnected systems and devices.[9]

As set forth in FTA and NIST guidelines, system integration and interoperability assessments are important for identifying compatibility limitations and determining whether AIM can reliably support current and future operational requirements. By not performing an integration assessment, WMATA reduced its ability to identify technical limitations, ensure AIM's compatibility with critical system interfaces, confirm the system's readiness, and determine whether it remains a dependable, cost-effective platform for ongoing rail operations and long-term infrastructure planning.

Overall, without basic continuity protections such as software escrow, technical solution assessments, and system integration reviews, WMATA has limited assurance that AIM will remain a reliable, supportable, and cost-effective supervisory control system capable of meeting current and future operational needs.

Recommendations

OIG recommends the GM/CEO:

1. Implement a long-term AIM replacement and continuity strategy that defines the future supervisory control platform, transition approach, key milestones, funding requirements, and contingency plans to maintain uninterrupted rail operations.

[8] *FTA. Project and Construction Management Guidelines. January 2025.*

[9] *NIST. Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0. February 2021.*

Management Response

Management concurs. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), the central cross-functional team will first establish an AIM baseline covering performance, capacity, reliability, maintainability, cybersecurity, lifecycle cost, and supportability, and will identify which deficiencies can be corrected through stabilization or optimization. During Phase 2 (Assess and Design), the team will complete an independent AIM feasibility and lifecycle assessment, informed by proportionate market research, peer-transit consultation, and a workforce assessment, and will compare sustainment, targeted modernization, and replacement options against documented requirements. The resulting options analysis will recommend a future-state course of action and an AIM continuity strategy, including the transition approach, key milestones, funding requirements, and contingency arrangements, for executive approval. The approved course of action will advance in Phase 4 (Modernize and Integrate). Progress will be tracked through the Program Management Office's integrated master schedule and corrective action register, and the analysis will not presume replacement, additional staffing, or a particular supplier.

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management’s comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

2. Establish software continuity protections by implementing a software escrow agreement and strengthening vendor contracts to provide access to source code, technical documentation, and other critical assets needed to maintain or restore AIM operations if vendor support becomes unavailable.

Management Response

Management concurs with the need for software continuity protections. Under Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy) and Objective 7 (Reduce Vendor and Key Person Dependency), the central cross-

functional team, Procurement, and other internal stakeholders will, during Phase 2 (Assess and Design), assess existing license and contract rights, source-code ownership, third-party dependencies, documentation completeness, and the build and restoration requirements needed to maintain or restore AIM operations if vendor support becomes unavailable. The team will evaluate software escrow or equivalent rights to source materials, technical documentation, recovery assets, and configuration information, including release conditions, deposit verification, update obligations, usability testing, cost, and enforceability. Continuity, documentation, access, performance, and transition requirements will be incorporated into future contracts and task orders. Execution of an escrow agreement will proceed once the assessment supports the arrangement and the required contractual and funding approvals are obtained.

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

3. Conduct an independent engineering and technology feasibility assessment of the AIM platform. Benchmark its performance, capacity, scalability, maintainability, lifecycle costs, and integration capabilities against current industry solutions. Use the results to determine whether AIM remains the most appropriate long-term supervisory control platform or should it be replaced.

Management Response
An independent engineering and technology assessment of the AIM platform will be completed. The planned Red Line CBTC and central SCADA environment is not intended to connect to or integrate with the existing AIM system. AIM sustainment and modernization for the Blue, Orange, Silver, Green, and Yellow (BOSGY) lines therefore remain a separate responsibility and investment need. References in this response to coordinated modernization mean coordination of operational readiness, infrastructure dependencies, resource decisions, and transition planning; they do not imply a direct

AIM-to-CBTC interface. The absence of that interface does not, by itself, establish that all transition or shared-infrastructure risks have been resolved. Management will document the relevant boundaries and evidence supporting its response to OIG. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), an independent engineering and technology assessment of the AIM platform will be completed in Phase 2 (Assess and Design).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

While the Management Response does not specifically state management's concurrence, the substance of its written response and the Strategic Plan nonetheless identify actions that are sufficiently responsive, if implemented, to address the recommendation. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 2: WMATA Has Not Effectively Managed Vendor and Key-Person Dependencies or Ensured Adequate Contract Oversight

WMATA currently lacks effective governance to address key-person dependency, over-reliance on the AIM vendor, and contract oversight for the AIM system. This has occurred because DM has not adopted best practices such as succession planning, cross-training, clearly defined vendor responsibilities, and contract verification procedures. Consequently, WMATA is exposed to potential risks to operational continuity, unnecessary costs, and duplicated efforts.

Specifically, OIG identified the following deficiencies:

a. **Vendor and Key-Person Dependency:** DM relies on one vendor and a single employee for specialized AIM configuration, troubleshooting, software support, system recovery, and AIM and train control interface support. Because AIM software is owned and maintained by [redacted] WMATA must depend on [redacted] for the software and specialized support. This reduces WMATA's ability to independently manage, support, and modernize the AIM system and creates an operational risk if the vendor support is disrupted.

   At the same time, much of WMATA's internal AIM operational knowledge and responsibilities are concentrated with one employee. This individual possesses much of the institutional knowledge required to support both WMATA and [redacted] and is also the primary resource responsible for maintaining AIM configuration data, assisting with system integrations, and resolving operational issues. This concentration of critical institutional knowledge creates a significant operational continuity risk if that employee becomes unavailable.

   Best practices outlined in COBIT 2019 recommend several strategies to enhance operational resilience and continuity. These include identifying critical roles, documenting institutional knowledge, implementing cross-training, defining vendor responsibilities, and managing vendor dependencies.[10]

   Contrary to this guidance, DM has not established a plan to transfer knowledge, conduct cross-training, or define operational responsibilities for AIM between WMATA and [redacted] The concentration of critical operational knowledge and specialized support responsibilities creates uncertainty about WMATA's ability to maintain AIM operations if

[10] *COBIT 2019 Framework: Governance and Management Objectives - APO07.03, Personnel Skills and Competencies; BAI08, Managed Knowledge; APO10.01/.03/.04/.05, Vendor Relationships, Contracts, Risk, and Performance; DSS04.02/.06, Business Resilience and Continuity Training.*

key personnel become unavailable or vendor assistance is disrupted. This situation increases the likelihood of delayed issue resolution, prolonged service disruptions, reduced organizational resilience, continued vendor dependence, and diminished operational and modernization readiness.

b. **Insufficient Oversight of Vendor Responsibilities and Task Order Pricing:** WMATA lacked sufficient contract oversight and task order pricing controls to ensure that [redacted] compensation reasonably reflected the work performed by [redacted] personnel and not by WMATA employees. DM senior personnel identified instances in which WMATA employees performed work included in [redacted] task orders. For example, this included two task orders (one valued at approximately $947,057 for the Virtual Machine Mesh Network Upgrade and $47,071 for an AIM operating system upgrade), both of which involved work by WMATA staff. For the Virtual Machine Mesh Network Upgrade, WMATA maintained insufficient oversight to identify which activities were performed by [redacted] versus WMATA personnel, or the level of effort contributed by each party. Consequently, OIG could not determine the full extent of any potential overpayment.

   COBIT 2019 recommends that organizations establish effective governance over third-party service providers by clearly defining responsibilities, validating deliverables, monitoring performance, and ensuring technology expenditures provide measurable value.

   As a result of not adequately documenting the division of work, WMATA risks unnecessary expenditures, potential vendor overcompensation, and reduced value from its AIM investment when a vendor receives task order payments despite WMATA employees performing project work.

c. **Duplicate Equipment Procurement:** WMATA independently procured, configured, and installed duplicate equipment for two capital projects at the Van Dorn (J03) location. This occurred because WMATA departments had not coordinated project scopes, reconciled overlapping work activities, or verified that vendor task orders and equipment purchases were not duplicated before work was authorized and completed.

   OIG reviewed the Van Dorn system configurations with DM personnel, showing that system changes implemented in fiscal year (FY) 2025 were performed under the ATC Renewal Project for COSI and the Power Tagging Relay Project for Power. For each project, WMATA independently procured and installed separate RTUs, Programmable

Logic Controllers, and other ancillary hardware because COSI and Power did not communicate and coordinate effectively on the two projects. In addition, DM personnel informed OIG that similar duplication exists at approximately 24 locations along the Blue, Yellow, and Green Lines.

COBIT 2019 guidance recommends coordinated project management, effective vendor and contract oversight, lifecycle management of critical assets, and appropriate budget and cost controls to ensure technology investments are managed effectively and deliver the expected value.[11]

Weak project governance in this area has contributed to overlapping capital investments, duplicate work, and project complexity. As a result, WMATA has limited assurance that its investment decisions are effectively coordinated, cost-effective, and deliver the greatest operational value.

Collectively, these conditions reduce WMATA's ability to sustain critical AIM operations, effectively manage vendor performance and contract expenditures, and ensure capital investments are coordinated and deliver the intended operational value. They also weaken vendor accountability and financial oversight, increase unnecessary costs, and reduce the effective use of public resources needed to support reliable rail operations and future modernization initiatives.

Recommendations

OIG recommends the GM/CEO:

4. Establish a workforce and operational continuity strategy to reduce key person dependency and strengthen in-house expertise in AIM operations, operational data management, OT communications, and systems integration necessary to support long-term rail modernization.

Management Response

Consistent with Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency), Digital Modernization will strengthen the capabilities of the core AIM Support Team (2 Technical Leads, 1 Application Specialist, 1 Developer) so that it can scale to support the system. Management will identify critical roles, competencies, single points of knowledge, and succession risks; develop competency matrices for AIM operations, databases, OT

[11] *COBIT. 2019 Framework: Governance and Management Objectives. §§ BAI11; APO10; BAI09; APO06; and EDM02.*

communications, systems integration, cybersecurity, and configuration management; and assign trained primary and backup personnel for critical functions. Structured knowledge transfer, cross-training, and readiness demonstrations will be required, with critical cross-training and knowledge-transfer activities completed in Phase 3 (Implement Priority Controls). Additional positions or training obligations will be proposed only where the workforce assessment demonstrates a need.

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
While the Management Response does not specifically state management's concurrence, the substance of its written response and the Strategic Plan nonetheless identify actions that are sufficiently responsive, if implemented, to address the recommendation. OIG will follow up on the planned actions during the corrective action plan phase.

5. Strengthen vendor and contract oversight by enforcing clear responsibilities, validating vendor deliverables and invoices before payment, implementing performance and cost controls.

Management Response
Management concurs with the need to strengthen vendor and contract oversight. Current controls include COTR vendor reviews, delineation of responsibilities between WMATA personnel and contractors, validation of work in lower environments, and approval before contractor work is implemented in the production environment. Under Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency), management will further clarify WMATA and vendor responsibilities in contracts and task orders and require validation of deliverables, labor hours, materials, and invoices before payment. Existing validation controls continue under Phase 1 (Mobilize and Stabilize), and contract oversight and cost recovery procedures will be strengthened in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

6. Strengthen project management governance and oversight by implementing centralized coordination, reconciliation, and labor hour validation controls to prevent duplicative work and unnecessary payments.

Management Response

Management concurs. Under Strategic Plan Objective 1 (Establish Executive Governance and Accountability), the Program Management Office will provide centralized coordination of AIM-related work through the integrated master schedule, decision log, dependency map, and corrective action register so that overlapping or duplicative activities are identified before work is authorized. Under Objective 4 (Strengthen Configuration and Change Management), project deliverables, database changes, labor hours, and field implementation records will be reconciled before payment approval. These controls build on existing COTR vendor reviews, delineation of WMATA and contractor responsibilities, lower-environment validation, and production approval. Validation controls continue under Phase 1 (Mobilize and Stabilize) and will be strengthened in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 3: WMATA Relies on Outdated RTUs and Legacy Communications Infrastructure

WMATA relies on outdated Remote Terminal Units (RTUs) and aging communications infrastructure to support AIM's supervisory monitoring and control functions. Many of WMATA's RTUs are no longer vendor-supported and beyond their intended service life. In addition, most RTUs communicate over a legacy Data Transmission System (DTS) network, which is older and less reliable than modern fiber-based communications. Although WMATA launched the Train Control Room (TCR) Renewal Project (CIP 0251_15) to replace outdated RTUs and the Master Fiber Project to upgrade communications, it has made little progress on either. Collectively, these conditions reduce the reliability of supervisory monitoring and control, increase the likelihood of equipment and communications failures, delay modernization efforts, increase lifecycle costs, and weaken project oversight and investment accountability.

OIG made the following observations:

a. **Outdated RTUs**: RTU reliability is essential to maintaining continuous supervisory monitoring and control of operationally critical equipment across the rail network. RTUs and the supporting communications infrastructure connect the AIM system to critical field equipment across the rail network, including traction power, tunnel ventilation, pumps, fans, and station equipment. However, many of WMATA's RTUs are outdated. Although they are still operational, the equipment is no longer vendor-supported and has surpassed its intended service life.

   Of the 110 stations and yards, 91 (83%) have outdated RTUs, which means only 17% are equipped with modern, vendor-supported units. *(see* **Table 1**).

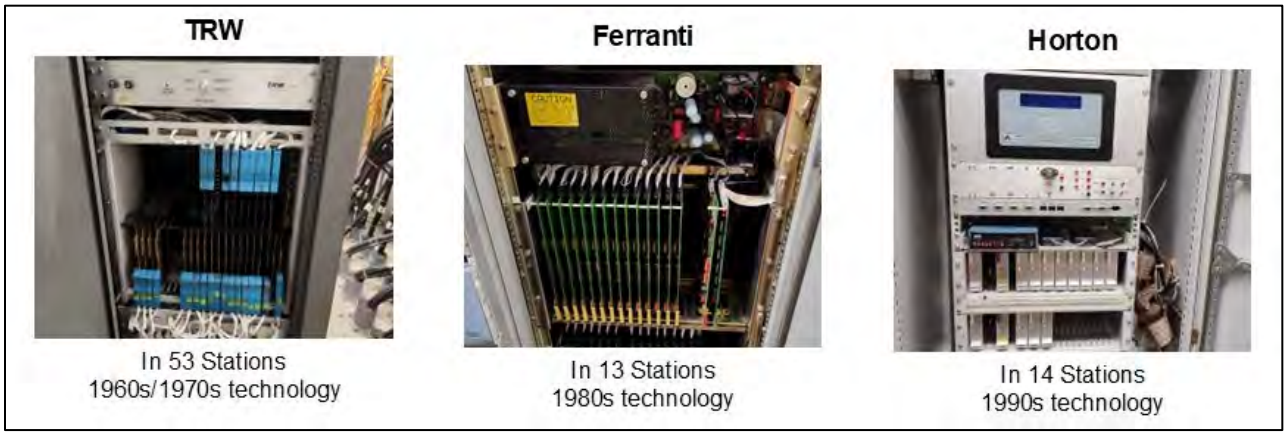
Table 1: ATC RTUs by WMATA Route - 83% of RTUs Are Outdated (30 - 60 Years Old)

Outdated RTUs by WMATA Route					
Route	**Rail Line(s) Included**	**# Stations or Yards**	**# with Outdated RTU**	**% with Outdated RTU**	**# Outdated but Planned for Upgrade**
A	Red	16	15	94%	2
B	Red	14	12	86%	0
C	Yellow, Orange, Silver, Blue	16	14	88%	1
D	Orange, Silver, Blue	14	13	93%	1
E	Yellow, Green	11	10	91%	1
F	Yellow, Green	12	11	92%	0
G	Silver, Blue	5	5	100%	0
J	Blue	2	2	100%	1
K	Orange, Silver	9	9	100%	3
N	Silver	11	0	0%	0
Total (All Routes)	**Total (All Rail Lines)**	**110**	**91**	**83%**	**9**

110 total stations and yards include duplicates for Metro Center, L'Enfant Plaza, Fort Totten, and Branch Ave, which are included in multiple routes. There are 106 distinct stations and yards.

WMATA RTUs are primarily composed of decades-old hardware from manufacturers that no longer provide support for these technologies. Despite this, WMATA continues to rely on three obsolete RTU models: TRW units from the 1960s-1970s, Ferranti units from the 1980s, and Horton units from the 1990s (*see* **Figure 2**).

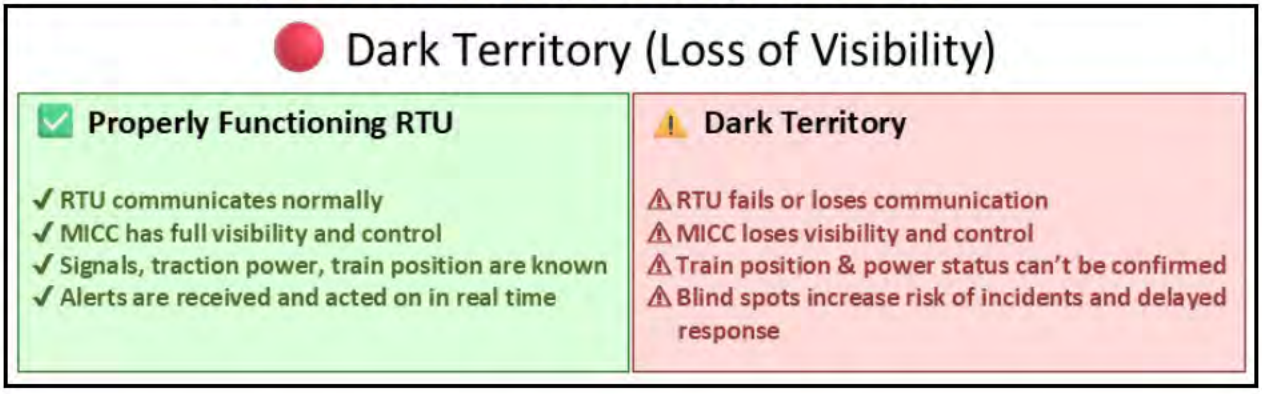
Figure 2: Types of Legacy RTUs in Use



OIG observed a pattern of operational instability across the older RTU population. From 2022 to 2025, data revealed 96 RTUs failed 334 times, averaging 3.5 failures per unit. Systemwide, this equates to an RTU failure approximately every four days, with a mean time between failures of 4.2 days. Notably, the 15 RTUs with the highest failure rates malfunctioned more than three times the rate of the rest of the fleet, averaging 8.20 failures each, compared with 2.60 for the remaining 81 units. When an RTU fails, it creates a condition commonly referred to as “Dark Territory.” This condition occurs when the MICC loses visibility or control over portions of the rail system. As a result, operational

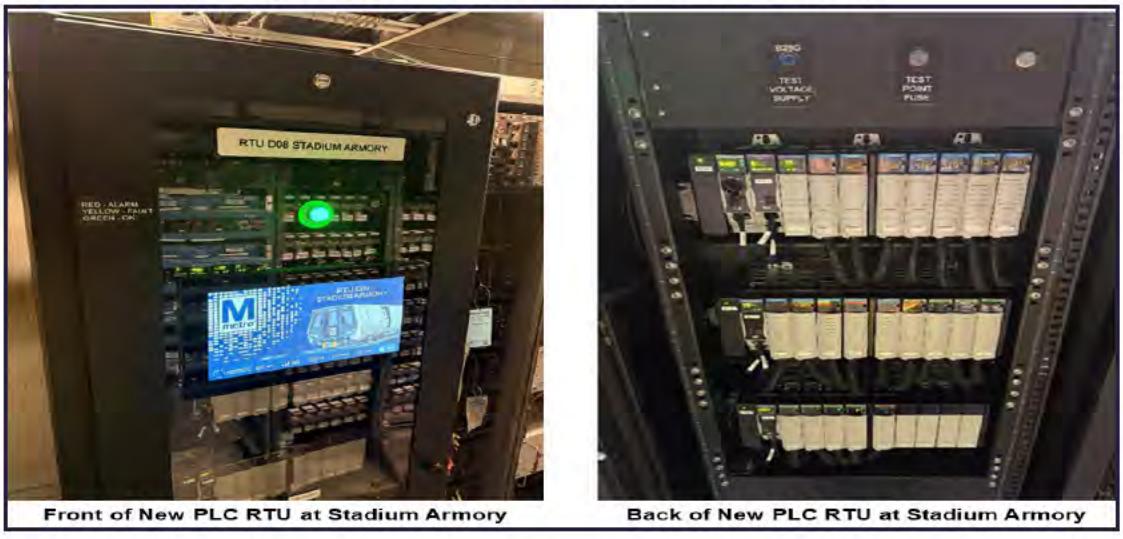
blind spots are created that increase the risk of service disruptions, delayed response to operational events, and potential safety incidents. **Figure 3** contrasts a properly functioning RTU with normal communication and full system visibility against Dark Territory conditions.

Figure 3: Dark Territory Caused by Outdated RTU



As of the end of FY 2026, WMATA had upgraded or replaced RTUs at 19 Metrorail stations and yards, including the N-Route/Silver Line and C11/Potomac Yard. These locations primarily use newer, vendor-supported Alstom Vital Processor Interlocking (VPI), Hitachi, and Allen-Bradley Programmable Logic Controller (PLC)-based RTUs (*see* **Figure 4**). These locations primarily use newer, vendor-supported Alstom VPI, Hitachi, and Allen-Bradley Programmable Logic Controller (PLC)-based RTUs.

Figure 4: New PLC RTU at Stadium Armory



Front of New PLC RTU at Stadium Armory | Back of New PLC RTU at Stadium Armory

The FTA TAM Rule[12] requires FTA grant recipients – including WMATA – to systematically manage capital assets throughout their lifecycle, assess asset condition and risks, and prioritize investments to achieve and maintain a SOGR and support safe and reliable transit operations. Further, FTA provides guidance to transit providers in its *TAM Systems Handbook*,[13] which emphasizes the importance of lifecycle asset management, condition and performance monitoring, and investment prioritization to manage system degradation and failure risks and support safe and reliable transit operations. Effective lifecycle management, modernization planning, and timely replacement of degraded or obsolete assets are essential to maintaining system reliability and reducing operational and lifecycle risks.

By not prioritizing RTU modernization, WMATA does not align with the FTA rule or guidance. Despite plans to upgrade RTUs, WMATA has not accelerated or prioritized the replacement of outdated RTUs based on factors such as their condition, failure history, operational criticality, lifecycle risk, and location. As these aging RTUs continue to deteriorate and fail, operational disruptions become more frequent, increasing the likelihood of Dark Territory conditions. Consequently, these failures reduce system reliability and complicate future modernization efforts. Furthermore, as vendor support declines, obtaining spare parts becomes increasingly difficult, which further complicates equipment maintenance.

b. Ineffective Cost Tracking for Upgrading RTUs: In 2021, WMATA began replacing outdated RTUs through the Train Control Room (TCR) Renewal Project to improve the reliability of the AIM environment and support critical rail infrastructure. However, the project did not include dedicated line items to track RTU modernization costs, preventing WMATA from identifying how much was spent specifically on RTU upgrades.

CIP 0251_15 had a total budget of approximately $49.54 million, with approximately $25.67 million spent as of FY2026. To evaluate modernization spending, OIG requested detailed RTU expenditure information from COSI's budget manager on multiple occasions but did not receive any documentation identifying RTU-specific costs.

---

[12] FTA 49 CFR Part 625, Transit Asset Management, §§ 625.5, 625.17, 625.25, 625.33, and 625.41 2026. Among other things, the FTA TAM rule required FTA grantees to develop asset management plans for their public transportation assets, including vehicles, facilities, equipment, and support infrastructure.

.

[13] FTA TAM Systems Handbook: Focusing on the Management of Our Transit Investments, September 2020, Section 5, "Systems Performance Management and Investment Prioritization," Pages 85 - 89. The "handbook is intended to expand upon and provide general information and guidance on the management of systems and associated assets used in the transit operating environment in support of the FTA TAM rule. It offers a framework that outlines systems theoretical concepts and defines specific classes and types of transit systems to foster consistency in transit system asset management practices." Handbook at 3.

According to the Government Accountability Office (GAO) Cost Estimating and Assessment Guide (GAO-20-195G):

> Project costs should be identifiable, traceable, and adequately documented to support effective cost management, oversight, and independent validation. Consistent with these principles, COBIT 2019 guidance[14] recommends establishing financial transparency and monitoring technology investments to ensure project costs are accurately tracked, reported, and managed throughout the investment lifecycle.[15]

Because RTUs are mission-critical assets, modernization expenditures should be clearly identified, tracked, and monitored to ensure financial transparency, effective oversight, and responsible stewardship of public funds. When these expenditures are not properly tracked, WMATA cannot fully account for modernization spending, weakening transparency and management accountability. This lack of cost visibility limits WMATA's ability to monitor modernization progress, evaluate investment performance, and increases the risk of cost overruns, duplicate spending, misallocated funds, and ineffective planning for future upgrades.

c. **Reliance on Legacy Data Transmission System (DTS) Network**: Approximately 94 percent of RTU connections to control devices still operate on the outdated legacy DTS, a copper-based communications network. The DTS network has limited bandwidth and capacity, which restricts data throughput, scalability, and system performance. In contrast, fiber optic connections eliminate bottlenecks, reduce lag, support future growth, resist environmental interference, and make unauthorized data access far more difficult.

   COSI and Power staff stated that WMATA relies on DTS to connect control devices, such as traction power, tunnel ventilation, pumps, fans, breakers, and other equipment, to the AIM supervisory control system. Further, the COSI ATC engineer indicated that the current architecture limits their ability to operate these control devices at its full capability. Additionally, Power staff informed OIG that delays in completing the DTS-to-Fiber Upgrade Project prevent the MICC from fully automating third-rail power operations, upgrading RTUs, and tagging relay systems from operating at full capacity.

---

[14] *COBIT 2019 Framework: Governance and Management Objectives-Detailed Guidance.*

[15] *GAO. Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Program Costs. GAO -20-195G.*

FTA's TAM *Systems Handbook* states that system managers must act to ensure interoperability between newer and legacy system elements in dynamic environments.[16] In addition, FTA's Communications-Based Train Control (CBTC) Systems Report (Report No. 0045) emphasizes that CBTC architectures rely on deterministic, high-speed, and redundant fiber-optic communications to support CBTC and connectivity among critical train control systems.[17]

WMATA has an ongoing DTS-to-Fiber Upgrade Project; however, progress has lagged, and the project remains incomplete. Delays in the DTS-to-Fiber Upgrade Project hinder newly installed equipment from functioning correctly or at optimal levels and increase the risk of project delays, additional costs, and integration challenges, which may impede other modernization efforts, including the Red Line CBTC Program.

Completing the DTS-to-Fiber Upgrade Project is therefore critical to improving operational reliability, strengthening system resilience, and ensuring long-term readiness for future modernization initiatives, including the Red Line CBTC Program.

Recommendations

OIG recommends the GM/CEO:

7. Implement a comprehensive RTU modernization strategy that accelerates replacement of aging RTUs, prioritizes upgrades based on asset condition, failure history, operational criticality, and lifecycle risk, and improves system reliability through enhanced visibility and automation.

Management Response

The central cross-functional team will coordinate an Infrastructure-led assessment of RTU inventory and condition, failure history, communications coverage, operational criticality, supportability, security capabilities, integration constraints, and existing approved project scope. Market research will compare feasible equipment and communications options, lifecycle support, interoperability, installation requirements, maintenance skills, and total ownership cost. Peer-transit consultation will examine migration sequencing, testing, outage management, and lessons from legacy field-equipment modernization. Engineering and safety review will determine where laboratory validation or a controlled field pilot is needed

[16] *FTA, TAM Systems Handbook: Focusing on the Management of Our Transit Investments, September 2020. Pages 98-100.*

[17] *FTA. An Assessment of the Business Case for Communications-Based Train Control. FTA Report No. 0045. September 2013. Page 88.*

before scaling. The team will recommend a prioritized and costed stabilization and modernization roadmap, with scope and acceleration decisions reserved for the required approvals.

Accountable Organization(s): Infrastructure – Communications & Signaling, Digital Modernization – Operational Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
While the Management Response does not specifically state management's concurrence, the substance of its written response and the Strategic Plan nonetheless identify actions that are sufficiently responsive, if implemented, to address the recommendation. OIG will follow up on the planned actions during the corrective action plan phase. In particular, OIG understands that Strategic Plan Objective 3 (which includes "[i]mplement[ing] a coordinated, risk-based program to replace obsolete RTUs and accelerate fiber connectivity") will be part of management's planned actions during that phase.

8. Implement controls to clearly identify, track, and report RTU upgrade costs within the TCR Renewal Project budget and strengthen budget governance through complete expenditure documentation and dedicated RTU line-item reporting.

Management Response
The actions necessary to address this recommendation are encompassed within the corrective actions established for Recommendation 7. Accordingly, these actions will be implemented and tracked through the same coordinated approach to avoid duplicative efforts. This aligns with Strategic Plan Objective 3, which provides for evaluating dedicated RTU budget line items and expenditure controls and for separately tracking and reconciling RTU expenditures.

Accountable Organization(s): Infrastructure – Communications & Signaling

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

While the Management Response does not specifically state management's concurrence, the substance of its written response and the Strategic Plan nonetheless identify actions that are sufficiently responsive, if implemented, to address the recommendation. OIG will follow up on the planned actions during the corrective action plan phase.

9. Accelerate completion of the DTS-to-Fiber Upgrade Project by prioritizing fiber connectivity to high-risk and critical rail locations and aligning RTU modernization efforts to restore system visibility, reduce dark territory conditions, improve operational reliability, and support the successful implementation of the Red Line CBTC program.

Management Response

Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 7 to avoid duplicative effort. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure), RTU replacement will be coordinated with the DTS-to-Fiber Upgrade Project, and fiber connectivity will be prioritized for critical and high-risk rail locations to restore system visibility and reduce dark territory conditions. Priority locations will be identified in Phase 1 (Mobilize and Stabilize), initial fiber priorities will be executed in Phase 3 (Implement Priority Controls), and modernization will expand in Phase 4 (Modernize and Integrate). Coordination with Rail Modernization will address shared infrastructure and transition dependencies relevant to the Red Line CBTC program.

Accountable Organization(s): Infrastructure – Communications & Signaling, Rail Modernization, Digital Modernization – Operational Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

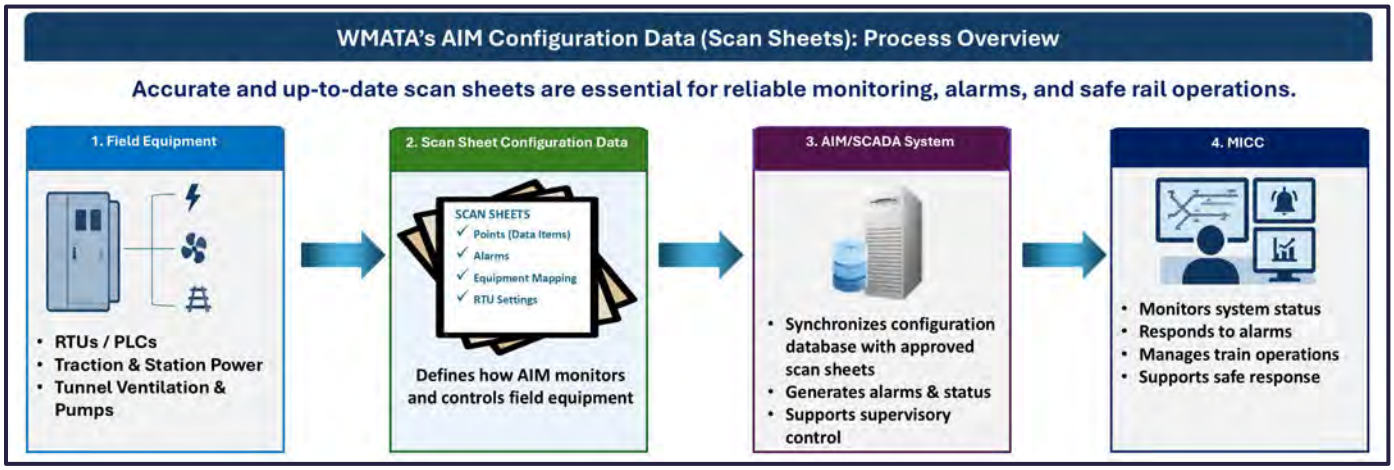
OIG considers management’s comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 4: WMATA Does Not Effectively Manage Critical AIM Configuration Settings

WMATA lacks effective governance and management controls of AIM configuration settings. AIM relies on detailed configuration settings to correctly interpret equipment status, generate alarms, and display real-time operational information to the MICC. Scan sheets document the configuration settings that define how AIM monitors and controls field equipment, processes alarms, and displays equipment status on MICC monitoring screens. AIM maintains these settings in its own production database, which should remain synchronized with approved scan sheet configurations and actual field conditions. WMATA does not consistently review, validate, reconcile, test, or approve changes to scan sheet configuration before implementing them in AIM. WMATA also lacks a single authoritative repository for scan sheets and does not integrate scan sheet configuration risks into its Safety Risk Management (SRM) process. As a result, WMATA cannot ensure that AIM configuration data remains accurate, complete, and aligned with actual field conditions.

a. **Lack of Governance Over Scan Sheets**: The process WMATA uses to review, validate, and approve scan sheets before they are implemented in AIM is ad hoc and is not consistently applied across departments. COSI, Power, and other responsible departments must ensure scan sheet configuration data is updated when field equipment is decommissioned, replaced, removed, or modified. **Figure 5** illustrates the intended workflow for reviewing, reconciling, approving, and submitting scan sheet changes to [redacted] for incorporation into the AIM production environment.

Figure 5: WMATA's AIM Scan Sheet: Process Overview



OIG found that WMATA does not consistently follow this workflow, and approval practices vary across departments. According to Power and COSI personnel, when scan sheet updates are required, they submit the scan sheets to DM for approval, and DM then forwards them to [redacted] for implementation. The level of review and the required supporting documentation differed depending on the department initiating the scan sheet change. Additionally, the roles and responsibilities for reviewing, reconciling, approving, and validating changes to scan sheets were neither clearly defined nor consistently applied across departments.

AIM relies on its operational configuration database to ensure live information received from field equipment is correctly identified and displayed to the MICC. The database should reflect approved scan sheet information and actual field conditions. Scan sheets that were not properly reviewed and approved may lead to incorrect information being displayed at the MICC. For example, at the West Falls Church traction power substation, OIG found scan sheet changes that had not been properly reviewed, approved, or incorporated into the AIM operational configuration database. When an AIM network failure occurred, the system reverted to the existing AIM production[18] configuration rather than the changes reflected in the updated paper scan sheets. This meant that the AIM system incorrectly displayed two circuit breakers as closed when they were physically open. This created a mismatch between AIM and actual field conditions and could have affected MICC's ability to accurately determine breaker status during the network failure.

Both NIST Special Publication, 800-53, Revision 5,[19] (CM-9) and NIST Special Publication 800-128,[20] which address Configuration Management, recommend formal governance and oversight with clearly defined roles, responsibilities, and approval authorities. These guidelines also call for organizations to document, review, test, and approve configuration changes before implementing them in the operational environment.

Contrary to the NIST guidance, WMATA has not implemented governance that requires independent review, testing, reconciliation, or formal approval before changes are placed into service. As a result, the MICC may receive false or untimely operational information, which can cause missed or delayed alarms and unsafe operational information and conditions on the rail.

---

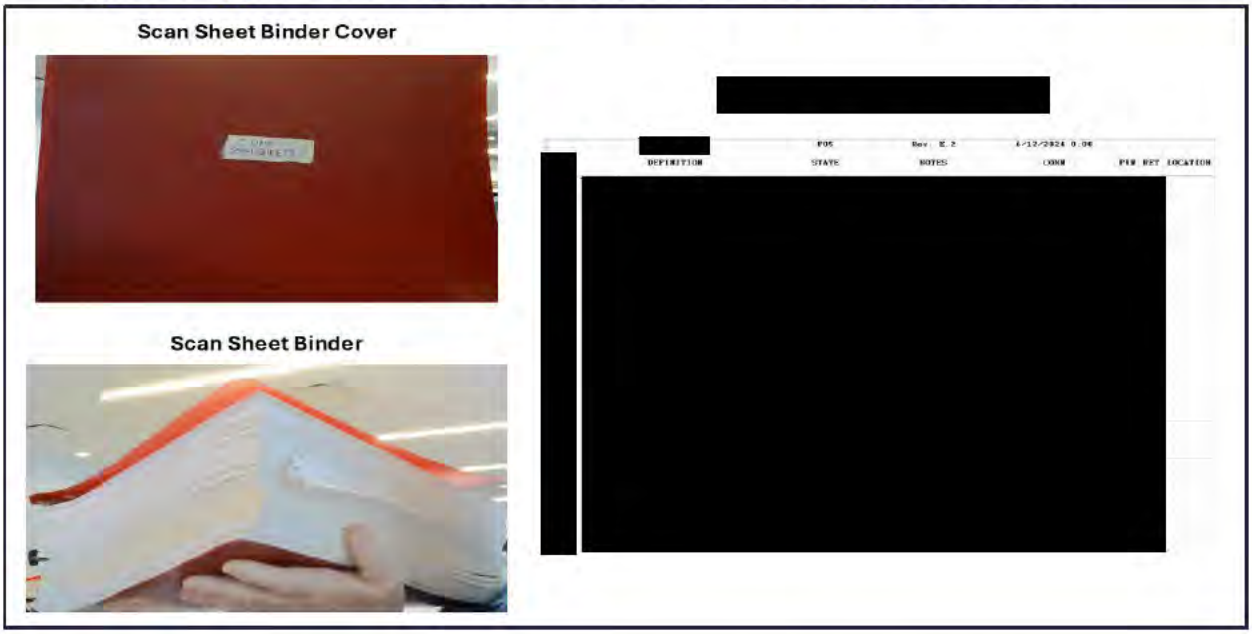
[18] *AIM Production refers to the live AIM systems that support WMATA rail operations, as distinguished from development and testing environments.*

[19] *NIST. Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Revision 5. September 2020. Pages 110-111.*

[20] *NIST. Special Publication 800-128: Guide for Security-Focused Configuration Management of Information Systems. Pages 11–12 and 36–37.*

b. **Lack of a Single, Reliable Source for Managing Critical Scan Sheets**: AIM scan sheets are stored in multiple locations (physical binders, SharePoint, shared drives, Procore),[21] and maintained in multiple formats (Excel, PDF, hard copy). This inconsistent and decentralized storage prevents WMATA from maintaining a single, reliable source for scan sheets and increases the risk of errors. For instance, OIG observed that outdated scan sheets contained in physical binders were still being used for current configuration activities (*see* **Figure 6**).

Figure 6: Typical WMATA Scan Sheet Binder and Sample Scan Sheet



Further, a sample of COSI scan sheets for ATC showed that some had not been updated, reviewed, revised, or recertified for over eight years. A defined update and review process is critical for WMATA to determine if scan sheets reflect current field conditions or remain necessary.

WMATA's Public Transportation Agency Safety Plan (PTASP)[22] requires the identification of safety-significant operational processes, associated hazards, and risk controls. The Plan also requires agencies to conduct a formal engineering review, independent validation, testing, management approval, and reconcile configuration changes. Despite these requirements, DM has not established a formal process to ensure independent review, version control, reconciliation with field equipment, documented validation, or

[21] *Procore serves as one of WMATA's key project management software repositories. Projects for Metro Rail are stored in Procore.*
[22] *WMATA. Public Transportation Agency Safety Plan, Version 6.0. December 31, 2025.*

certification before deploying scan sheet configurations to AIM's production environment. DM personnel stated that WMATA lacks a centralized process to update and reconcile AIM configuration data when field equipment is modified, replaced, or removed from service. As the department responsible for managing AIM and its databases, DM has not established controls to ensure the production database remains synchronized with approved scan sheets and actual field conditions.

Because scan sheet configuration data are not maintained in a single authoritative repository, multiple versions of the same scan sheet may exist across different platforms, making it difficult to determine which data are current and accurate. This decentralized and unstandardized storage increases the risk that outdated or unsupported configurations remain active within the AIM database, including inactive equipment records, duplicate or conflicting device configurations, outdated system information, unmonitored equipment conditions, and inconsistent alarm settings. These conditions limit WMATA's ability to verify the completeness and accuracy of AIM configuration data and ensure alignment with current field conditions.

c. **WMATA's Safety Risk Management (SRM) Process Lacks Scan Sheet Safety Risk Assessments**: WMATA has not incorporated AIM scan sheet configuration changes, associated hazards, or configuration safety risks into its SRM process. Since scan sheets determine how AIM displays equipment status, alarms, and supervisory monitoring information, configuration-related risks should be identified and managed through WMATA's SRM process before implementing configuration changes in AIM. However, DM has not established a process to ensure that this occurs.

   FTA regulations under 49 CFR § 673.25 require public transportation agencies to establish an SRM process to identify hazards, assess safety risks, and implement appropriate mitigations.[23] WMATA implements these requirements through its PTASP, which establishes Metro's SRM process and includes Management of Change as part of the framework for evaluating safety risks associated with changes that could affect operations.[24] These requirements provide a framework for identifying, assessing, and mitigating safety risks from AIM configuration changes before implementation, helping prevent unaddressed risks to rail operations and personnel safety.

[23] *49 CFR Part 673.25, Safety Risk Management.*

[24] *WMATA, Public Transportation Agency Safety Plan, Version 6.0, Section 3.0, "Safety Risk Management." December 31, 2025. Page. 27; Section 3.5, "Management of Change."*

Without conducting such a review, safety risks associated with AIM configuration changes may not be identified, assessed, and mitigated before implementation. Configuration changes could then result in AIM incorrectly monitoring, controlling, or displaying the status of field equipment, alarms, and operational events. This inaccuracy could affect MICC operational decisions, including traction-power isolation, alarm response, and field equipment control, and increase safety risks to personnel.

Recommendations

OIG recommends the GM/CEO:

10. Establish a centralized AIM scan sheet configuration and database integrity program that requires that (a) scan sheet changes be reviewed, validated, reconciled with field equipment, formally approved through a change control board, and (b) scan sheets be periodically monitored to ensure configuration accuracy, integrity, and reliability.

    Management Response
    Management concurs. Consistent with Strategic Plan Objective 4 (Strengthen Configuration and Change Management), Digital Modernization will serve as technical owner of a centralized AIM configuration management program and authoritative repository for all scan sheets and configuration records, with ATC, SCADA Engineering, and Ventilation accountable for review and validation within their operational domains. Undocumented production changes, except emergency actions, will be frozen in Phase 1 (Mobilize and Stabilize); configuration standards, decision rights, and escalation procedures will be established in Phase 2 (Assess and Design); and the centralized repository, baseline controls, and Change Control Board (CCB) governance will be implemented in Phase 3 (Implement Priority Controls). Configuration changes will require independent review, field reconciliation, testing, documented validation, and CCB approval before production implementation, and scan sheets will be periodically audited and recertified.

    Accountable Organization(s): Digital Modernization – Operations Technology

    The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

11. Strengthen project coordination and accountability controls to prevent duplicate or conflicting scan sheet configurations and ensure AIM modernization activities, labor hours, and database changes are properly reconciled, validated, and aligned with approved project and contractual requirements.

Management Response

Management concurs. Consistent with Strategic Plan Objective 1 (Establish Executive Governance and Accountability) and Objective 4 (Strengthen Configuration and Change Management), Digital Modernization will implement project governance controls, coordinated through the Program Management Office, that require departments, project teams, and contractors to reconcile scan sheet changes, labor hours, project deliverables, and database modifications before implementation and payment approval. Management will maintain configuration baselines, track approved changes through the decision log and dependency map, validate implementation results, and conduct periodic configuration audits and recertifications to identify and resolve duplicate, conflicting, or unauthorized configurations. These controls will be implemented in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

12. Document AIM scan sheet governance, validation, reconciliation, and configuration management activities within WMATA's PTASP and Safety Risk Management processes and establish appropriate controls to monitor and mitigate associated operational risks.

Management Response
Management concurs. Consistent with Strategic Plan Objective 4 (Strengthen Configuration and Change Management) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Safety will incorporate AIM scan sheet governance, validation, reconciliation, and configuration management activities into WMATA's PTASP, Safety Risk Management, and Management of Change processes. Configuration changes that may affect supervisory monitoring, alarm functionality, equipment status, or operational control will require a documented safety risk assessment before deployment. Safety will document mitigation requirements, approval authorities, validation procedures, and ongoing monitoring, with Digital Modernization supporting as technical owner. Success will be measured by safety-significant configuration changes receiving documented risk review before deployment.

Accountable Organization(s): Safety and Readiness – Safety (Lead), Digital Modernization as technical owner

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 5: WMATA Lacks Effective AIM Operational Data Governance and Management

WMATA lacks effective AIM operational data governance and management practices needed to ensure that AIM operational and historical data remain accurate, complete, and reliable. WMATA's key AIM operational data management activities, including AIM database backup, synchronization, historian data management, operational reporting and analysis, database integrity, and operational baseline management, remain largely informal and manual and depend on a limited number of individuals with specialized knowledge.

Effective operational data governance and management are critical to WMATA's train control systems because accurate and reliable data support supervisory monitoring, alarm response, maintenance, and operational decision-making. For AIM, this includes clear ownership, responsibilities, standards, and controls for how real-time and historical data are collected, maintained, analyzed, and used. The AIM historian database[25] stores historical operational data for troubleshooting, reporting, performance monitoring, and trend analysis. A mature data management platform can also consolidate data for standardized reporting and analytics, key performance indicators (KPI) monitoring of system performance and reliability, and predictive analysis to identify emerging issues before they affect operations. These capabilities support reliable train control operations, informed decision-making, and WMATA's future rail modernization and Red Line CBTC readiness.

COBIT 2019 APO14.01 (Managed Data)[26] recommends that organizations establish a formal data management strategy, assign clear roles and responsibilities, and manage data as a critical organizational asset. NIST Special Publication 800-53, Revision 5,[27] also recommends controls to maintain the integrity, availability, and recoverability of operational data, including information integrity (SI-7),[28] system backup and recovery (CP-9),[29] and documented baseline configurations (CM-2).[30] Together, these practices provide a framework for formal data governance, defined responsibilities, data integrity, backup and recovery, and operational baseline management necessary to maintain reliable operational data.

---

[25] A historian database (or data historian) is a system used to capture and manage time-series data from an industrial control environment, that is, to record sequential measurements over time to permit an organization to track changes, identify trends, and analyze operational performance.

[26] COBIT 2019 Framework: Governance and Management Objectives (APO14.01): Define and communicate the organization's data management strategy and roles and responsibilities. Pages 143-144.

[27] NIST. Special Publication 800-53: Security and Privacy Controls for Information Systems and Organizations. Revision 5. September 2020.

[28] SI-7, Software, Firmware, and Information Integrity. Pages 345–348.

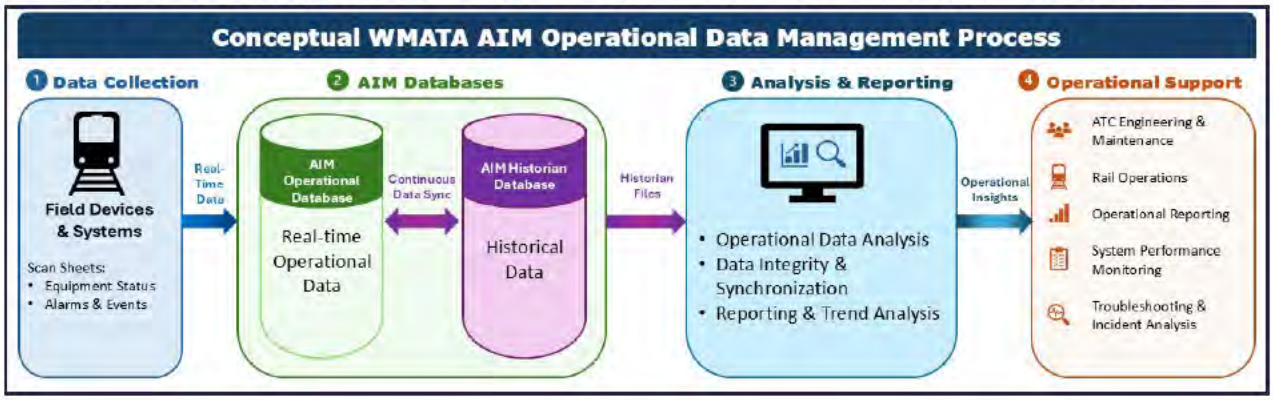
[29] CP-9, System Backup, Pages 125-127.

[30] CM-2, Baseline Configuration, Pages. 95-97

Inconsistent with best practices, WMATA management has not established formal governance over AIM operational data, including documented procedures, clear ownership and accountability, and effective oversight of database management, reporting, and analytics. Roles and responsibilities among [redacted] DM, and OT also remain unclear. In addition, WMATA relies on a limited number of personnel with specialized knowledge of AIM and data management to perform key activities. Formal governance should include automated controls to strengthen data integrity, synchronization, reconciliation, and operational baseline management.

According to NIST and COBIT, operational data should flow from field devices through the AIM real-time and historian databases to analysis, reporting, and operational support (*see* **Figure 7**). These processes support reliable rail operations, informed decision-making, system performance monitoring, system modernization, and long-term operational objectives.

Figure 7: Conceptual WMATA AIM Operational Data Management Process



In contrast to Figure 7, WMATA performs AIM database functions through informal, manual processes. In addition, WMATA remains heavily dependent on a small number of personnel with specialized knowledge in areas such as database backups and synchronization, historian data management, operational reporting, database integrity, operational baseline management, operational analysis, and AIM data interpretation. This reliance creates a fragile support structure and increases the risk of operational disruptions.

Collectively, these weaknesses reduce WMATA's ability to ensure that AIM operational and historical data remain accurate, complete, and reliable. Reliance on informal, manual processes increases the risk of human error and delays in identifying and correcting data integrity and synchronization issues. Dependence on a limited number of personnel with specialized AIM knowledge also creates continuity risks when those individuals are unavailable. These

weaknesses can reduce the reliability of operational monitoring, reporting, performance analysis, and decision-making, and limit WMATA's ability to support long-term rail modernization and the successful implementation of the Red Line CBTC program.

Recommendations

OIG recommends the GM/CEO:

13. Establish a formal AIM operational data governance and database integrity program with defined roles and responsibilities, standardized procedures, documented knowledge transfer and cross-training, and controls for backup, synchronization, reconciliation, historical data management, and operational baseline management.

    Management Response
    Management concurs. Under Strategic Plan Objective 5 (AIM operational data governance and management), existing backups will be validated and a priority restoration test performed in Phase 1 (Mobilize and Stabilize), and the daily database backups, hourly transaction log backups, and twice-daily historian archives will be evaluated based on recoverability evidence. In Phase 2 (Assess and Design), the central cross-functional team will complete a data assessment and establish governance standards defining data ownership and stewardship, standardized procedures, synchronization and reconciliation controls, retention and historical data management, operational baseline management, and documented knowledge transfer and cross-training. Success will be measured by successful backup and restoration testing and by the assignment of an owner and steward to each critical dataset.

    Accountable Organization(s): Digital Modernization – Operations Technology

    The estimated completion date is: TBD Pending Confirmation of Funding

    OIG Comment
    OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

14. Implement a centralized AIM data management platform that has the ability to consolidate operational and historical data and support standardized reporting and analytics, KPI monitoring of system performance and reliability, and predictive analysis to improve operational and maintenance decision-making and Red Line CBTC readiness.

Management Response

Management concurs with the need for improved reporting, KPI monitoring, and analytics. These actions will be implemented and tracked with the corrective actions for Recommendation 13. Consistent with Strategic Plan Objective 5, operational and maintenance stakeholders will define reporting use cases, KPI definitions, and predictive-analysis needs during Phase 2 (Assess and Design), and market research and peer-transit benchmarking will compare enhancing existing tools with adding a centralized platform. Any approved centralized AIM data management and analytics capability will be implemented in Phase 4 (Modernize and Integrate), subject to the approved assessment and business case, with AIM/BOSGY and Red Line needs assessed separately.

Accountable Organization(s): Rail Modernization, Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 6: WMATA Lacks Effective AIM Alarm Management, Root Cause Analysis, and System Performance Monitoring

AIM alarms are not accurately prioritized, analyzed, monitored, and resolved to support reliable rail operations and informed operational decision-making. WMATA lacks a formal alarm management program, structured root cause analysis procedures, and centralized system performance monitoring necessary to identify, prioritize, analyze, mitigate, and track recurring alarm and system performance issues affecting the AIM environment. As a result, WMATA lacks a comprehensive view of system reliability, recurring performance issues, and operational conditions that may affect rail operations and future modernization efforts.

OIG identified the following control weaknesses affecting AIM alarm management, root cause analysis, and monitoring practices:

a. **Ineffective Alarm Management** – MICC operators rely on AIM alarms and supervisory monitoring information to identify abnormal operating conditions, respond to hazards, manage traction power and train control operations, and maintain operational awareness across the rail network. Current alarm management efforts have focused primarily on suppressing or partitioning alarms rather than fully identifying and correcting the root cause. Specifically, nuisance alarms,[31] chattering alarms,[32] and fleeting alarms,[33] are not properly resolved and managed. In some instances, operators may inhibit or suppress these alarms without proper authorization.

   Between May 2025 and April 2026, WMATA's *Weekly Top Ten AIM Alarms Reports* showed that approximately 15,000 to 45,000 alarms, across 565 unique alarm categories, were generated each week, most of which were nuisance alarms. These alarms repeatedly transition between active and inactive states, resulting in chattering alarms. This clutters the AIM alarm display and can make it more difficult for the MICC controllers to identify which alarms require attention. The high volume of chattering, fleeting, and other nuisance alarms can overwhelm controllers, reduce operational awareness, and hinder timely response to critical events and abnormal conditions. Many of these excessive alarms are generated by traction power equipment due to intermittent communication issues associated with the legacy DTS copper communications network.

[31] *Nuisance alarms - An alarm that occurs excessively or unnecessarily or remains active after the appropriate operator's action has been taken.*

[32] *Chattering alarms - An alarm that repeatedly switches between an active and inactive state within a short period.*

[33] *Fleeting alarms - An alarm that briefly switches between active and inactive states but, unlike a chattering alarm, does not rapidly repeat.*

American National Standards Institute/International Society of Automation (ANSI/ISA) 18.2 standard[34] provides an industry framework for managing alarms throughout their lifecycle, including alarm identification, rationalization,[35] prioritization, monitoring, maintenance, and performance assessment. These practices are intended to reduce nuisance alarms and excessive alarms and to ensure that operators receive meaningful, actionable alarm information. Effective alarm management helps MICC controllers identify abnormal conditions, prioritize critical alarms, and respond promptly to operational issues.

WMATA does not maintain effective governance, access controls, or monitoring over the AIM alarm inhibition and suppression functions. Alarm inhibition or suppression temporarily prevents selected alarms from being presented to operators when operationally appropriate, such as during authorized maintenance, testing, or abnormal operating conditions. WMATA has not implemented planned software partitioning and access restrictions intended to limit these functions to authorized personnel and operational groups in the AIM production environment. Likewise, WMATA does not conduct alarm rationalization as defined by ANSI/ISA. Without these controls, WMATA has limited assurance that alarms are inhibited or suppressed only when authorized and operationally appropriate.

b. Inadequate Root Cause Analysis – DM provided OIG with WMATA's Operational Technology Incident Management Plan and sample AIM outage incident reports to demonstrate how they resolve outage incidents. The reports document event timelines, immediate technical causes, operational impacts, and short-term corrective actions. However, the reports do not consistently identify and analyze the underlying causes contributing to recurring AIM issues and supervisory monitoring deficiencies.

Recurring AIM alarms, communication failures, inactive signals, outages, and other supervisory monitoring issues are not consistently analyzed, escalated, tracked, investigated, or corrected through a formal root cause analysis and remediation process. In addition, incident documentation does not consistently include trend analysis, pattern identification, corrective action validation, or other follow-up needed to determine whether root causes were corrected, recurring patterns were identified, and similar incidents were prevented. Lack of coordination among DM, COSI, Power, MICC, and other responsible

---

[34] ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries, Section 5, Alarm Management Lifecycle, pp. 28–30; Section 9, Rationalization; Section 16, Monitoring and Assessment; and Section 18, Audit.

[35] ANSI/ISA-18.2 standard provides that rationalization in this context "is the systematic process of reviewing, justifying, and documenting potential or existing alarms to ensure each one is truly needed, properly prioritized, and actionable for operators."

departments also limits WMATA's ability to consistently identify and resolve the root causes of AIM outages and operational failures.

ANSI/ISA-62443-2-1[36] provides a framework for managing incidents affecting industrial control systems, including incident analysis, corrective actions, and measures to reduce recurrence. These practices support effective root cause analysis. Without effective root cause analysis and coordinated response among stakeholders, recurring AIM outages, communication failures, alarm problems, and other supervisory monitoring issues may remain unresolved or recur. This will increase troubleshooting and maintenance efforts and reduce the reliability of AIM monitoring and control operations.

c. **Lack of AIM Monitoring and Performance Metrics** – The AIM system generates millions of operational data elements each day, providing real-time information on alarms, equipment performance, communication status, and operator actions that can be used to monitor system health. WMATA has not established standardized AIM performance metrics, defined Key Performance Indicator (KPI) thresholds, centralized dashboards, or routine management reporting necessary to provide management with a comprehensive view of system performance, reliability, and operational risks. WMATA is developing a data warehouse environment to receive AIM operational data and support future reporting, performance metrics, trend analysis, analytics, and integrated operational monitoring. However, these capabilities remain under development and have not yet matured into a fully governed and integrated operational data management, analytics, and reporting program.

   Specifically, we identified the following weaknesses in WMATA's monitoring and reporting of AIM system performance:

   - **Alarm Performance Monitoring -** WMATA has not established performance targets, thresholds, or routine management reporting for AIM alarms. Weekly Top Ten AIM Alarms Reports are manually produced and do not provide consistent reporting on overall alarm volumes, recurring alarm categories, trends, or overall alarm performance. As a result, WMATA cannot readily determine whether alarm conditions are improving, deteriorating, or creating operational risks that require corrective action.

[36] *ANSI/ISA-62443-2-1 (99.02.01)-2009, Security for Industrial Automation and Control Systems, Part 2-1: Establishing an Industrial Automation and Control Systems Security Program. Pages 144-145.*

- **RTU and Field Device Performance Monitoring –** WMATA has not established routine performance monitoring and management reporting for RTU availability, communication reliability, recurring failures, or equipment health trends. COSI performs annual RTU testing and receives alarms when RTU communications fail. However, engineers manually gather and compile performance information from AIM, maintenance records, and field personnel, and AIM does not generate automated performance reports. Performance monitoring, therefore, remains largely ad hoc, limiting management's ability to identify reliability trends, deteriorating equipment, and priorities for corrective action or replacement.

ANSI/ISA-18.2[37] and COBIT 2019 MEA01[38] recommend that organizations establish performance measures, monitor and assess system performance, identify and trend recurring issues, define accountability, and provide management reporting necessary to support reliable operations. WMATA has not implemented effective performance monitoring to help management identify, assess, and resolve recurring operational issues.

Without effective AIM alarm performance monitoring, WMATA may not identify recurring alarm problems, declining equipment performance, and reliability issues before they affect operations. This can lead to reactive maintenance, delayed corrective action, and increased risk of service disruptions and reduced AIM reliability.

Weak alarm management, root cause analysis, and AIM performance monitoring limit WMATA's ability to identify and resolve recurring alarm, communication, and equipment problems before they affect rail operations. As a result, problems may persist, corrective actions may remain reactive, and emerging reliability risks may go undetected. These weaknesses reduce assurance that AIM can reliably support rail operations, emergency response, and future modernization.

Recommendations

OIG recommends the GM/CEO:

15. Establish a formal AIM alarm management process with designated personnel, roles, and responsibilities to improve alarm design and control, including alarm governance, rationalization, prioritization, threshold management, and suppression and partitioning controls.

[37] *ANSI/ISA-18.2-2016, Management of Alarm Systems for the Process Industries, March 2016. Pages 26-30*

[38] *COBIT 2019 Framework: Governance and Management Objective - MEA01, Managed Performance and Conformance Monitoring, Page 273.*

Management Response
Management concurs. Consistent with Strategic Plan Objective 6 (Improve Alarm Management, Reliability, and Root Cause Analysis), MICC and technical domain owners, coordinated through the central cross-functional team, will establish an AIM alarm management philosophy and governance standard in Phase 2 (Assess and Design) that designates personnel, roles, and responsibilities and defines alarm rationalization, prioritization, threshold management, and suppression and partitioning controls. The assessment will address alarm inventory, nuisance and recurring conditions, operator workload, response procedures, and escalation criteria, informed by peer-transit practices. Engineering and Safety will review operational consequences and define testing, approval, rollback, and monitoring requirements; changes will not be justified solely by reducing alarm volume. Priority alarm rationalization will be implemented in Phase 3 (Implement Priority Controls), and alarm performance will be continuously improved in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

16. Perform a comprehensive review and rationalization of AIM alarms to identify, correct, and monitor nuisance and excessive alarm conditions affecting AIM reliability and operational awareness.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15. Consistent with Strategic Plan Objective 6, a comprehensive alarm rationalization will identify and correct chattering, fleeting, stale, duplicate, and recurring alarms, with priority rationalization completed in Phase 3 (Implement Priority Controls). Results will be monitored through the Strategic Plan's Performance Dashboard,

including alarm volume, nuisance-alarm percentage, and repeat alarms, and improved continuously in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

17. Implement appropriate access restrictions and monitoring controls over AIM alarm inhibition, override, partitioning, and suppression functions to ensure these functions are used only by authorized personnel.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15 and the access control actions for Recommendation 25. Consistent with Strategic Plan Objective 6 and Objective 8 (Strengthen Cybersecurity and Access Controls), AIM alarm inhibition, override, partitioning, and suppression functions will be restricted to authorized roles, privileged alarm actions will be centrally logged, and those logs will be periodically reviewed. These controls will be implemented in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

18. Establish a formal AIM root cause analysis process with defined escalation criteria, cross-functional coordination among DM, COSI, Power, MICC, and other responsible stakeholders, centralized tracking, and corrective action accountability to identify and resolve underlying causes and prevent recurring AIM operational problems.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15. Consistent with Strategic Plan Objective 6, RCA standards will be established in Phase 2 (Assess and Design), defining escalation thresholds for significant outages, communications failures, alarm floods, and recurring events and assigning cross-functional responsibilities among DM, COSI, Power, MICC, and other responsible stakeholders. Centralized RCA and corrective action tracking will be implemented in Phase 3 (Implement Priority Controls), with corrective actions tracked through verified closure and reported through the Performance Dashboard's RCA completion and corrective action closure measures.

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling (COSI), Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

19. Establish a formal AIM performance monitoring and reporting program with standardized performance measures, KPIs, and routine management reporting to monitor alarm performance, AIM reliability, and RTU and field equipment performance and health.

Management Response
Management concurs. Consistent with Strategic Plan Objective 6 and the Strategic Plan's Performance Dashboard, Digital Modernization will establish an AIM performance monitoring and reporting program that defines performance measures, KPI thresholds, reporting responsibilities, and governance requirements. KPI baselines and executive dashboards will

be established in Phase 2 (Assess and Design) and will cover AIM availability and major outage trends; RTU availability, failure rate, and replacement progress; alarm volume, nuisance-alarm percentage, and repeat alarms; and RCA completion and corrective action closure. Routine management reporting will use these results to prioritize corrective actions, modernization investments, and reliability improvements.

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications & Signaling, Infrastructure – Power, Infrastructure – Facilities, Metro Integrated Command Center

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 7: Physical Access Controls to Critical Train Control Rooms Need Strengthening

WMATA does not maintain adequate physical security over its TCRs, which house critical communications equipment, supervisory control interfaces, network components, and power systems that support rail operations. Access to these rooms is not consistently controlled or monitored, and most locations lack access-point barriers and closed-circuit television (CCTV) surveillance. Access point controls and CCTV would enable WMATA to better manage and monitor access to the TCRs. Inadequate access and monitoring controls increase the risk of unauthorized access, equipment tampering, theft, and service disruption.

Physical Access to TCRs

[redacted] OIG did not receive evidence that physical-key access is consistently logged, monitored, inventoried, or periodically reconciled, limiting WMATA's ability to detect, investigate, and respond to unauthorized access attempts (*see* **Figure 8**).

Figure 8: Illustration of TCRs Using a Key or Cipher Lock for Entry



NIST Special Publication 800-53, Revision 5, recommends controls for restricting and managing physical access to facilities housing critical systems, maintaining physical access records, securing and inventorying physical access devices, and monitoring access to detect and respond to unauthorized activity.[39] Effective physical security over TCRs would include controlled issuance, asset logging, and periodic key reconciliation audits.

Weak key control for TCRs increases the risk that unauthorized individuals could access or tamper with rail equipment, cause operational disruptions, and create safety hazards. Without secure key management and access logs, WMATA cannot reliably track or monitor who enters these rooms, undermining accountability and system integrity.

Closed-Circuit Television (CCTV) Surveillance

[redacted]

Restricted and monitored access is essential to ensuring that only authorized personnel enter TCRs and that access is logged and traceable to support accountability, security oversight, and incident investigations.

Recommendations

OIG recommends the GM/CEO:

20. Conduct a cost/benefit analysis and risk assessment to determine the sufficiency of current security and access controls for TCRs. Based on that analysis, implement additional security and access controls, such as badge access readers and electronic access logging.

    Management Response
    Management concurs. Consistent with Strategic Plan Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Communications and Signaling, in coordination with the Metro Transit Police Department, Digital Modernization, and operating departments, will complete

[39] *NIST. Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, PE-2, Physical Access Authorizations; PE-3, Physical Access Control; and PE-6, Monitoring Physical Access. Pages 180-185.*

a risk assessment and cost-benefit analysis of Train Control Room (TCR) physical security controls in Phase 2 (Assess and Design), evaluating key management, access authorization, access monitoring, and surveillance coverage. Based on the results, risk-prioritized enhancements, such as electronic badge access, automated access logging, key inventory and reconciliation, and CCTV monitoring, will be implemented at priority locations in Phase 3 (Implement Priority Controls), with broader physical security improvements completed in Phase 4 (Modernize and Integrate). Periodic reviews of TCR access records and security controls will be established to sustain accountability.

Accountable Organization(s): Communications and Signaling (COSI), Digital Modernization, and MTPD support

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 8: Cybersecurity Controls Over AIM and Interfaced Train Control Systems Need Strengthening

WMATA lacks adequate cybersecurity governance, risk management, monitoring, and assurance to protect AIM and its interfaced train control systems.[40] This is because WMATA has not implemented controls suited for AIM's legacy architecture, outdated RTUs, legacy OT communication protocols, and extensive customizations. These weaknesses increase the risk of cybersecurity incidents that could compromise data integrity, disrupt system reliability and operations, and raise recovery and support costs.

OIG identified the following cybersecurity, network architecture, and governance deficiencies affecting the security and reliability of WMATA's AIM and its interfaced train control systems:

a. **AIM Cybersecurity Governance Plan Has Not Been Updated -** WMATA's current AIM cybersecurity program is defined in the Cyber Security Plan (CSP). This plan, developed by a vendor in July 2017, has not been updated to reflect how WMATA should implement and maintain cybersecurity governance, risk management, operational security controls, monitoring activities, and security responsibilities across the current AIM environment.[41]

   NIST publications – specifically, NIST Special Publication 800-82, Revision 3,[42] and NIST Special Publication 800-53, Revision 5[43] – establish cybersecurity best practices for OT systems, including maintaining current security plans, conducting risk assessments, implementing security controls, and conducting continuous monitoring to identify and manage evolving cyber risks. These best practices are required under WMATA's Cybersecurity Policy (P/I 15.28/0), including periodic updating to address a changing cybersecurity risk environment.

   The outdated CSP increases the risk that security controls and OT protections may not address evolving cyber threats, operational changes, and vendor dependencies. These conditions reduce management assurance that the AIM environment is consistently governed and protected against cybersecurity threats and operational disruptions.

---

[40] Interfaced train control systems include train and field devices, traction power systems, and communication protocols, such as DNP3, used to connect these systems to AIM.

[41] The AIM environment includes monitoring operations, interfaces with critical operational infrastructure, including traction power, ventilation, pumps, breakers, and other operational technology systems supporting daily Metrorail operations.

[42] NIST. Special Publication 800-82, Revision 3: Guide to Operational Technology (OT) Security. Pages 38, 55-56, and 93.

[43] NIST. Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems. Page 216.

b. [redacted]

WMATA Cybersecurity Manual requires that the CISO implement "industry standard best practices," including the globally recognized standards by the Center for Internet Security (CIS).[44] CIS standards provide that secure baseline configurations, system hardening, encryption, vulnerability management, security testing, and evaluation of software changes to reduce cybersecurity vulnerabilities.

Despite these requirements and standards, [redacted] Without these controls, DM has limited assurance that [redacted] This increases the risk of unauthorized access, credential compromise, ransomware, system compromise, and service disruptions affecting critical rail supervisory monitoring operations.

c. Legacy Communication Protocols and Outdated RTUs Increase Cybersecurity Risks – [redacted]

NIST Special Publication 800-82, Revision 3, which addresses security controls within OT systems, recommends layered cybersecurity controls, including secure communications, authentication, encryption, system hardening, and integrity protections to reduce cyber risks.[45]

[44] CIS is a U.S. nonprofit organization that creates globally recognized cybersecurity standards, such as the CIS Controls and CIS Benchmarks, to help secure IT systems and data.

[45] NIST Special Publication 800-82 Revision 3 Guide to Operational Technology (OT) Security September 2023, Section 5.2, Defense-in-Depth Architecture Capabilities, pages 78, 207, 224, addressing layered security across management, physical, network, hardware, and software controls.

Reliance on aging RTUs and legacy communication protocols increases the risk of unauthorized commands, spoofing, data manipulation, and disruption of critical rail monitoring and control functions.

d. AIM Network Defense-in-Depth Controls Need Strengthening – DM's approach to layered security includes firewalls, Virtual Local Area Networks (VLANs), intrusion detection system, and a Demilitarized Zone[46] to control network traffic and separate network components within the AIM environment. DM stated that the AIM network is air-gapped, meaning AIM operates without a direct connection to the Metro web or the internet.[47] These controls are intended to protect rail operations from external cyber threats. However, DM's current security architecture lacks [redacted]

Both APTA SS-CCS-RP-002-13[48] and NIST Special Publication 800-82, Revision 3,[49] recommend defense-in-depth and network segmentation to protect critical operational systems. Defense-in-depth uses multiple layers of security controls to maintain protection when a single control fails. For example, APTA's recommended transit security zone architecture separates life-safety, operational, business, and external systems into controlled zones. These zones restrict unauthorized access, isolate critical rail functions, and help prevent cybersecurity incidents from spreading across systems.

DM has not established [redacted] Contrary to APTA and NIST guidance, DM does not [redacted]

These control weaknesses increase the risk that unauthorized access or compromise of one network segment could spread to critical AIM systems, disrupt rail operations, and reduce assurance that AIM is adequately protected against evolving cybersecurity threats.

e. User Access Controls Between AIM Environments Need Strengthening – DM did not consistently restrict user access or maintain a clear distinction among users of the various AIM development, test, and production environments. A review of Active Directory access

---

[46] A Demilitarized Zone (DMZ), according to the NIST CSRC Glossary, is a physical or logical network segment or host inserted as a "neutral zone" between an organization's private trusted network and untrusted external networks like the internet.

[47] NIST Computer Security Resource Center (CSRC) Glossary defines an air-gap as an interface where systems are not physically connected, and any logical connection is not automated.

[48] APTA-SS-CCS-RP-002-13 Defining Security Zone Architecture for Rail Transit & Protecting Critical Zones. Pages 15-30

[49] NIST Special Publication 800-82 Revision 3, Guide to Operational Technology (OT) Security. Pages 86 and 99.

reports and supporting documentation showed that both [redacted] and WMATA personnel maintained broad access across these environments.

NIST Special Publication 800-82, Revision 3,[50] and NIST Special Publication 800-53, Revision 5,[51] recommend role-based access controls and least-privilege access controls, separation of duties, and periodic access reviews and monitoring. The standards also call for development and test environments to be separated from production to prevent unauthorized access or changes to critical operational systems. Contrary to NIST guidance, DM did not conduct periodic reviews to ensure user access aligned with employee/contractor roles.

Weak access controls and insufficient separation among development, test, and production environments increase the risk of unauthorized access, system changes, cybersecurity compromises, and disruptions to critical rail operations.

Recommendations

OIG recommends the GM/CEO:

21. Update and maintain a current AIM cybersecurity governance program aligned with industry best practices such as NIST Special Publication 800-82 Revision 3, including defined security policies, standards, risk assessments, responsibilities, and monitoring requirements to support secure and reliable AIM operations.

Management Response

Management concurs. Consistent with Strategic Plan Objective 8 (Strengthen Cybersecurity and Access Controls), Digital Modernization – Cybersecurity will update and maintain an AIM cybersecurity governance program defining security policies, standards, risk assessment requirements, responsibilities, and monitoring requirements. Privileged and vendor access reviews will begin in Phase 1 (Mobilize and Stabilize). In Phase 2 (Assess and Design), the central cross-functional team and Cybersecurity will complete a cybersecurity assessment of control coverage, asset and network visibility, security boundaries, privileged and vendor access, server configuration, and legacy constraints, supported by a standards-applicability register referencing NIST SP 800-82 Revision 3, applicable CIS Windows Server guidance, and relevant APTA publications. AIM will continue to be managed as a subsystem within the

[50] NIST. Special Publication 800-82, Revision 3: Guide to Operational Technology (OT) Security, September 2023. Section 6.2.1, Access Control. Pages 100–104.

51 NIST, Special Publication 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations, AC-5 (Separation of Duties), AC-6 (Least Privilege), CM-2(6) (Development and Test Environments), and CM-4(1) (Separate Test Environments).

DM OT Boundary in Archer, with associated risks documented in the Risk Register. Enhanced controls will be deployed in Phase 3 (Implement Priority Controls) following compatibility assessment, safety and reliability review, testing, rollback planning, and approval.

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

22. [redacted]

Management Response
[redacted]

Accountable Organization(s): Digital Modernization – Cybersecurity

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

23. Modernize and secure legacy RTUs and communications supporting AIM through phased replacement and implementation of appropriate authentication, encryption, integrity protections, and other OT cybersecurity controls consistent with NIST guidance.

Management Response
Management concurs. These actions will be implemented through the RTU and communications modernization roadmap established for Recommendation 7. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure) and Objective 8 (Strengthen Cybersecurity and Access Controls), authentication, integrity, encryption, and logging controls will be incorporated into RTU and communications modernization where technically feasible, and cybersecurity testing will be required before operational acceptance. Implementation will follow the RTU and fiber sequence in Phase 3 (Implement Priority Controls) and Phase 4 (Modernize and Integrate), led by Infrastructure – Communications and Signaling in coordination with Digital Modernization.

Accountable Organization(s): Infrastructure - Communications and Signaling

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

24. Strengthen AIM cybersecurity by establishing and documenting defined security zones, effective network segmentation, layered security controls, and routine firewall rule reviews, consistent with APTA and NIST guidance.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8, Cybersecurity will define and document AIM security zones, segmentation requirements, approved communications paths, layered security controls, and firewall governance, informed by APTA and NIST guidance, and will conduct periodic firewall rule and segmentation reviews. Segmentation controls will be deployed in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: 12/31/2028

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

25. Strengthen AIM access controls by implementing role-based and privileged access management, separating development, test, and production environments, periodically reviewing user access, and restricting vendor access to critical operational systems.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8, Cybersecurity will implement role-based and privileged access controls based on least-privilege principles, separate development, test, and production environments, perform periodic user access reviews, and restrict and monitor vendor access to critical operational systems. Privileged and vendor access reviews will begin in Phase 1 (Mobilize and Stabilize), and enhanced access and privileged access controls will be deployed in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Cybersecurity

The estimated completion date is: 09/30/2027

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 9: WMATA Lacks Integrated Risk Management Over the AIM System

WMATA had not performed a comprehensive operational risk assessment to identify significant risks affecting rail operations. This occurred because WMATA has not established an effective governance and risk management framework to oversee the AIM supervisory control and monitoring platform. The lack of effective risk management limits WMATA's ability to identify, prioritize, and address and mitigate risks affecting the AIM and train control systems environment.

OIG identified governance and oversight weaknesses that affect WMATA's ability to manage AIM risks, including:

a. **Operational Risk Assessment** – When OIG requested the operational risk assessment, DM directed OIG to the Audit & Compliance department, which provided the risk registers. Upon reviewing the Risk Register, OIG found that it was missing crucial components necessary for an operational risk assessment of the AIM system. Key elements such as performance measures, escalation thresholds, and root cause analysis requirements were missing.

   NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*,[52] provides guidance for conducting risk assessments as part of an organization's overall risk management process. The guidance calls for organizations to identify and evaluate threats, vulnerabilities, likelihood, and potential impacts to operations and assets, and use the results to determine appropriate responses to identified risks. These practices provide a framework for WMATA to identify, assess, prioritize, and address risks that could affect AIM operations, reliability, and critical rail functions.

   DM has not established a comprehensive process to assess these risks or assurance activities to determine whether corrective actions were implemented and effective. Without a comprehensive operational risk assessment, WMATA has limited assurance that AIM risks are effectively managed and mitigated. Unaddressed risks could affect AIM reliability, service continuity, and safe rail operations.

b. **Asset Lifecycle, Vendor and Key-Person Dependency Risk Assessments** – The AIM environment continues to depend on aging RTUs, legacy communications infrastructure,

[52] *NIST. Guide for Conducting Risk Assessments, Special Publication 800-30, Revision 1. September 2012.*

customized, vendor-controlled software, and a limited number of personnel with specialized AIM knowledge. WMATA has not conducted formal lifecycle, vendor-dependency, or key-person risk assessments for AIM, even though AIM relies on specialized hardware, software, field equipment, and technical expertise essential to the supervisory monitoring and control of rail infrastructure.

FTA TAM regulations require WMATA to maintain a TAM plan that assesses asset condition and prioritizes investments needed to keep assets in good repair.[53] Similarly, COBIT 2019 establishes governance practices for managing asset lifecycle, vendor dependency, and key-person risks that could affect system reliability and modernization.[54] Together, these requirements and practices provide a framework for assessing asset condition and long-term supportability, managing vendor and workforce dependencies, and identifying modernization needs and risks.

Without formal risk assessments that align with these practices, WMATA is unable to make informed decisions about AIM replacement options, long-term supportability, vendor dependency risks, knowledge transfer needs, succession risks, modernization dependencies, or the impact of aging infrastructure on future operational and modernization objectives. As a result, WMATA has limited assurance that these risks are identified and effectively addressed. These gaps increase the risk of higher support costs, operational disruptions, and delays in modernization.

c. **Data Governance and Data Integrity Risk Assessments** – Modern rail systems increasingly rely on data as a foundation to drive operations. Accordingly, ongoing risk assessments of data quality, system integrity, and analytics capabilities are required to identify and mitigate operational risks. However, WMATA has not completed a comprehensive risk assessment of the AIM data environment. This includes evaluating risks associated with AIM historical data management, data quality controls, database integrity, RTU configuration baselines, scan sheet reconciliation, and alignment of operational data with actual field conditions. Each of these elements is a core component of the AIM system, which is necessary to ensure AIM's real-time accuracy.

   DM stated that WMATA performs AIM database backup, synchronization, replication, and recovery activities and is developing data lake and data warehouse capabilities to improve

[53] *FTA. Transit Asset Management (49 CFR Part 625), National Transit Asset Management System, § 625.25, Transit Asset Management Plan Requirements.*

[54] *COBIT. 2019 Framework: Governance and Management Objectives BAI09, Managed Assets Page 209; APO10, Managed Vendors Page 119; APO07, Managed Human Resources Page.*

reporting, analytics, and information sharing. Although WMATA had taken these steps, OIG found that WMATA lacked the necessary data architecture, technical capabilities, governance processes, and operating model to effectively manage operational data from RTUs, rail vehicles, wayside systems, and facility equipment. In addition, WMATA has not evaluated the workforce's capabilities or knowledge-dependency risks associated with AIM data management.

COBIT 2019 (APO14 – Managed Data and BAI09 – Managed Assets) recommends that organizations establish effective data governance, maintain reliable information assets, manage data throughout its lifecycle, and ensure technology assets provide accurate information to support business decisions.[55] Effective data governance and integrity risk assessments are necessary to ensure operational data remains accurate, reliable, accessible, and capable of supporting system monitoring, maintenance decisions, and future rail modernization.

Without effective data governance, data quality, and integrity risk assessments aligned with these standards, WMATA has limited assurance that AIM operational data is accurate, reliable, and ready to support current operations and future rail modernization. This limits WMATA's ability to use operational data for analytics to drive operational improvements, predictive maintenance, asset lifecycle decisions, and preparation for data-dependent technologies, such as the Red Line CBTC program and other future rail modernization efforts.

d. Long-Term RTU Risk Assessment – WMATA currently operates a combination of older and newer RTU infrastructure using fiber and copper communication media. The OIG found no comprehensive assessment that evaluated the long-term role of legacy ATC RTUs infrastructure.

COBIT 2019 (BAI03 and BAI09.01),[56] NIST Special Publication 800-82 Revision 3,[57] and FTA TAM guidance[58] recommend that organizations assess technology assets, supporting infrastructure, operational dependencies, and lifecycle risks to ensure that critical systems remain reliable, supportable, secure, and aligned with future operational and modernization requirements.

---

[55] *COBIT. 2019 Framework: Governance and Management Objectives BAI09 – 209, APO14. Page 143.*

[56] *COBIT. 2019 Framework: Governance and Management Objectives BAI03. Page 169 and 209.*

[57] *NIST. Special Publication 800-8, Revision 3,. Guide to Operational Technology (OT) Security: Pages 1, 6, 33, and 118.*

[58] *FTA. TAM Systems Handbook. Pages 85 and 94.*

Without a comprehensive risk assessment of the RTU environment as recommended by best practices, WMATA has limited assurance that its current infrastructure and technologies represent the most reliable, supportable, and sustainable architecture to meet its future needs.

e. Cybersecurity Risk Assessment – As AIM has expanded over time, legacy technologies, industrial communication protocols, increased system integration, and vendor-supported components create evolving cybersecurity risks that require continuous assessments. DM did not have any cybersecurity risk assessment of the AIM environment.

NIST SP 800-82 Revision 3,[59] and ANSI/ISA 62443[60] recommend that organizations assess cybersecurity risks, validate defense-in-depth protections, manage access controls, and maintain layered security practices to protect critical operational technology systems throughout their lifecycle. Contrary to such guidance, WMATA had not completed cybersecurity risk assessments covering several critical AIM risk areas.

The absence of a formal assessment and effective controls prevents WMATA from identifying vulnerabilities in its system architecture, legacy technologies, access controls, vendor dependencies, customized software, and operational technology. Further, cybersecurity weaknesses stemming from aging technologies, access controls, vendor dependencies, software changes, and evolving threats may go undetected or unresolved.

Recommendations

OIG recommends the GM/CEO:

26. Establish a formal AIM operational risk assessment process aligned with best practices, with defined ownership, periodic risk reviews, mitigation tracking, and ongoing monitoring to ensure risks that affect AIM system reliability and rail operations are consistently identified, prioritized, and addressed.

[59] *NIST. Special Publication 800-82, Revision 3: Guide to Operational Technology (OT) Security. Pages 41, 90, 94, 197, and 278.*

[60] *ANSI/ISA. 62443-3-3: Security for industrial automation and control systems. Pages 12 and 56.*

Management Response
Management concurs. DM Cybersecurity Services (DMCS) has established a formal cybersecurity risk management framework in which AIM is identified as a subsystem within the DM OT Boundary in Archer, and AIM cybersecurity and operational risks are documented, assessed, tracked, and monitored in the Risk Register and linked to Key Risk Indicators (KRIs), Key Control Indicators (KCIs), mitigation activities, and Plans of Action and Milestones (POA&Ms). Consistent with Strategic Plan Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), these AIM risks will be linked to the Strategic Plan's consolidated risk register, which defines risk scoring, acceptance authorities, mitigation requirements, and review frequency and connects operational and cybersecurity risks to corrective actions and investment decisions. DMCS will perform periodic AIM risk assessments and reviews, monitor mitigation through completion, and maintain current risk ratings, owners, target dates, and status. Success will be measured by all high and critical risks having approved treatments and owners and by risk reviews completed on schedule.

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: 06/30/2027

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

27. Establish a formal AIM lifecycle, vendor dependency, and knowledge management risk assessment process to identify and address replacement needs, asset sustainability, vendor reliance, knowledge transfer, and workforce readiness needed to support reliable operations and future rail modernization.

Management Response
Management concurs. Consistent with Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Digital Modernization, in coordination with Cybersecurity, will implement a recurring lifecycle, vendor dependency, and workforce readiness risk assessment for the AIM environment, evaluating asset supportability, technology obsolescence, vendor reliance, workforce capabilities, succession risks, knowledge-transfer requirements, and related cybersecurity risks. Identified risks will be recorded in the consolidated risk register with

owners and treatments, and results will inform modernization, continuity, cybersecurity, workforce, and investment decisions through the annual strategy, lifecycle, risk, workforce, and architecture reviews conducted in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

28. Establish a formal AIM data governance, data quality, and integrity risk assessment process to identify and address risks related to data architecture, system integrity, analytics capabilities, workforce skills, and technology needs that could affect operational reliability and future modernization, including the Red Line CBTC program.

Management Response
Management concurs. Consistent with Strategic Plan Objective 5 (AIM operational data governance and management) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Digital Modernization, in coordination with Cybersecurity and Rail Modernization, will establish a periodic AIM data governance and data integrity risk assessment covering data quality, database integrity, configuration accuracy, data architecture, analytics capabilities, workforce competencies, and supporting technologies. Identified risks will be recorded in the consolidated risk register with documented mitigation plans and accountable owners. Rail Modernization will provide input on modernization priorities, integration requirements, lifecycle planning, and future-state operational needs, and, consistent with Objective 2, Red Line CBTC considerations will be addressed through validation of CBTC/SCADA scope, dependencies, and AIM/BOSGY requirements.

Accountable Organization(s): Digital Modernization – Operational Technology, Rail Modernization

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

29. Establish a comprehensive risk assessment for AIM RTUs and supporting communications infrastructure, identify and address lifecycle and integration risks, define the future-state architecture, and support reliable operations and future rail modernization.

Management Response

Management concurs. These actions will be implemented and tracked with the RTU and communications corrective actions for Recommendations 7 and 23. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Infrastructure – Communications and Signaling will complete RTU and communications risk assessments in Phase 2 (Assess and Design) to identify lifecycle and integration risks and will define a vendor-neutral future-state field communications architecture. Identified risks will be recorded in the consolidated risk register and linked to the prioritized RTU and fiber modernization roadmap.

Accountable Organization(s): Infrastructure - Communications and Signaling

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

30. Establish a comprehensive AIM cybersecurity risk assessment process to identify and address operational technology risks related to defense-in-depth, access controls, vendor dependencies, software security, and legacy technologies that could affect secure and reliable rail operations and future modernization.

Management Response

Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8 (Strengthen Cybersecurity and Access Controls) and Objective 9 (Integrate Enterprise Risk, Safety, and

Physical Security), the AIM cybersecurity assessment completed in Phase 2 (Assess and Design) will address defense-in-depth, access controls, vendor dependencies, software security, and legacy technology risks. Results will be documented in the Archer Risk Register, linked to the consolidated risk register, and tied to corrective actions and investment decisions, with periodic reassessments to keep the risk profile current.

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Finding 10: Red Line CBTC Migration Readiness is Limited by AIM Technical Deficiencies and the Lack of a Vendor-Neutral CBTC Reference and Integration Architecture

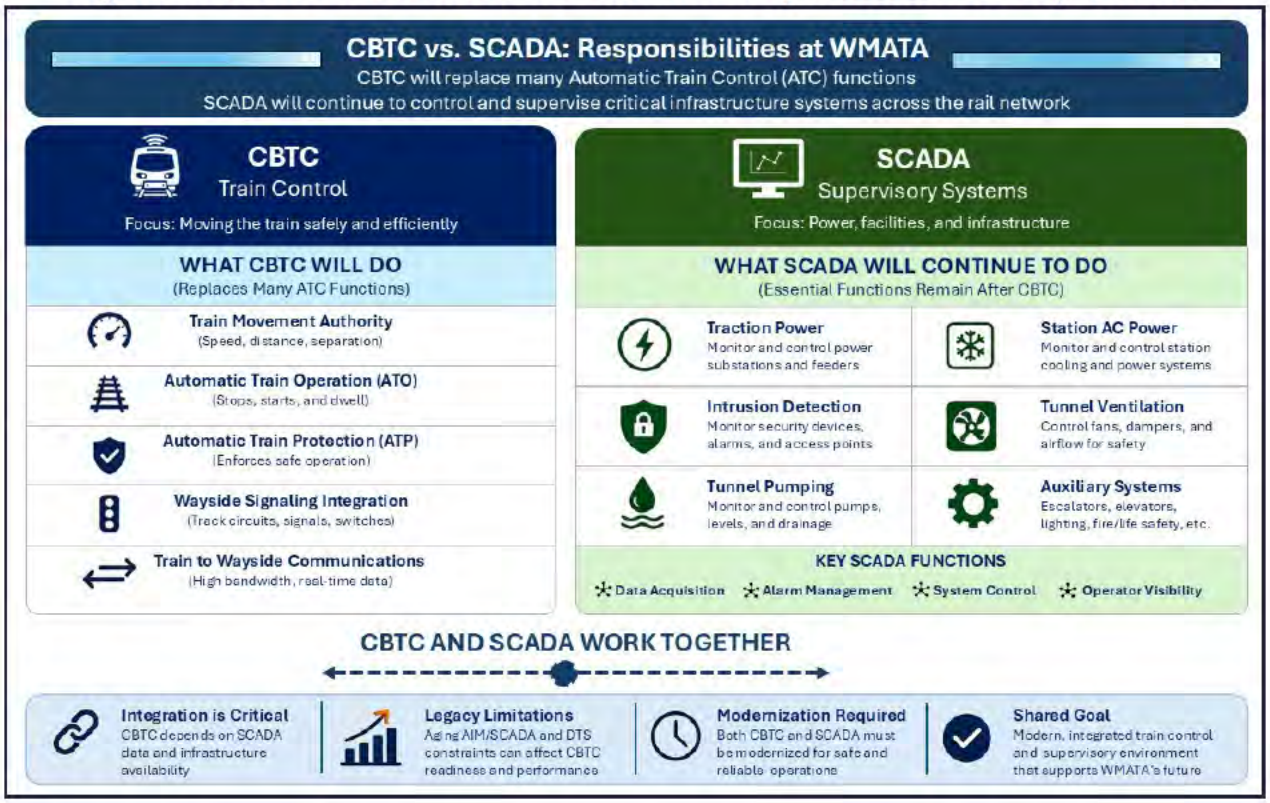
Longstanding deficiencies within the AIM environment present risks to WMATA's Red Line CBTC migration readiness. AIM provides foundational supervisory control and monitoring of critical rail infrastructure and will continue to support operations alongside the Red Line CBTC. Findings 1 through 9 identify deficiencies that WMATA needs to address, but has not yet addressed, as it transitions to CBTC (*see* **Appendix C**). In addition, WMATA has not established a vendor-neutral CBTC reference and integration architecture to define how AIM (or its successor) will integrate with the future CBTC environment. Together, these gaps limit WMATA's readiness for Red Line CBTC migration and increase integration, operational, cost, and schedule risks.

Because the AIM deficiencies identified during the audit present risks to CBTC integration and migration readiness, OIG expanded the audit scope to assess their potential effect on the transition to CBTC. OIG identified the following conditions that could affect the implementation and long-term performance of the CBTC program:

a. **AIM Governance and Technical Deficiencies Limit Red Line's CBTC Migration Readiness** – WMATA has not yet conducted a comprehensive modernization readiness and integration assessment to determine whether AIM and its supporting rail infrastructure can support the transition to CBTC. Addressing the deficiencies outlined in Findings 1 through 9, will help WMATA identify infrastructure limitations, system dependencies, integration requirements, and modernization needs before CBTC implementation.

   AIM reliability and modernization readiness are important to successful Red Line CBTC implementation. AIM will continue to provide supervisory control and monitoring of critical rail infrastructure, including CBTC, traction power, station power, ventilation, pumps, and other field systems (*see* **Figure 9**).

Figure 9: Illustration of AIM as a Foundational System for CBTC Operations



FTA Report No. 0045[61] highlights the integration between new CBTC equipment and existing control-center, legacy, and wayside systems as areas that should be addressed early in the process. Specifically, the report provides guidance for transit agencies implementing modern CBTC systems and explains that the primary challenges in CBTC upgrades stem from process and governance gaps. Based on lessons from CBTC upgrades at other transit systems, FTA recommends considering how existing and new systems will work together, defining requirements, and identifying interfaces early in the process.

For WMATA, this reinforces the need to assess and address the AIM deficiencies identified in Findings 1 through 9 as part of the Red Line CBTC transition. If WMATA does not do so, system or equipment failures could disrupt rail operations and limit the safety, reliability, and service improvements expected from the Red Line CBTC program.

[61] *FTA Report No. 0045, Executive Summary, An Assessment of the Business Case for Communications-Based Train Control (Sept. 2013). Pages 7-8.*

b. WMATA Has Not Yet Established a Vendor-Neutral CBTC Reference and Integration Architecture – The Red Line CBTC planning has focused primarily on procurement and vendor selection. However, there is no corresponding vendor-neutral CBTC reference and integration architecture that would define how the AIM system (or any successor) will integrate with the future CBTC operating environment, regardless of the vendor. A vendor-neutral reference and integration architecture would provide a WMATA-defined baseline for system interfaces, operational and data requirements, communications, traction power, MICC operations, cybersecurity, governance, and other dependencies independent of a specific vendor solution.

WMATA's Manual of Design Criteria (MDC)[62] establishes expectations for integration, including coordination across WMATA departments, Interface Control Documents for system interfaces, protection of existing operations during integration, and assessment of traction power requirements. OIG's preliminary research and inquiries did not identify a vendor-neutral reference and integration architecture or detailed architectural designs for the future CBTC environment. OIG also did not identify a documented architectural baseline that connects existing AIM systems, infrastructure, and operational dependencies to the MDC integration expectations and the future CBTC environment.

FTA Report No. 0045[63] emphasizes a systems engineering approach to CBTC implementation, including requirements development and validation, system integration, lifecycle considerations, and migration planning. These practices help identify system dependencies and integration requirements early, reducing operational, cost, and schedule risks during CBTC migration.

Without a defined, vendor-neutral architecture, WMATA has limited assurance that existing AIM dependencies and integration requirements will be identified and addressed before they become dependent on vendor-specific designs. This increases the risk of integration issues, design changes, vendor dependency, additional costs, implementation delays, and operational disruptions during CBTC migration.

AIM technical deficiencies and the lack of a defined CBTC reference and integration architecture increase integration, operational, cost, and schedule risks and limit assurance of a reliable and sustainable transition to Red Line CBTC.

---

[62] *WMATA. Manual of Design Criteria, Section 22.4.2.2, CBTC Integration.*

[63] *FTA. An Assessment of the Business Case for Communications-Based Train Control, Report No. 0045. 2013. Pages. 134139.*

Recommendations

OIG recommends the GM/CEO:

31. Conduct a formal CBTC modernization readiness and integration assessment to evaluate AIM technical debt, infrastructure dependencies, system interfaces, operational requirements, vendor and workforce dependencies, and other factors that could affect the transition to Red Line CBTC.

    Management Response
    Management concurs. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), Rail Modernization, supported by Digital Modernization – Operational Technology and coordinated through the central cross-functional team, will conduct a CBTC readiness and integration assessment in Phase 2 (Assess and Design). The assessment will validate Red Line CBTC/SCADA boundaries, required supervisory functions, field and communications dependencies, operational transition requirements, cybersecurity responsibilities, vendor and workforce dependencies, and the continuing AIM/BOSGY scope. It will document which AIM risks have no direct Red Line interface dependency, which affect continuing operations, and which shared or transition dependencies require action. Vendor-neutral market research and peer-transit consultation will inform requirements and acceptance criteria, and proposals will be reviewed against WMATA's Manual of Design Criteria and applicable industry requirements. The planned 2034 milestone and proposed procurement will not predetermine the outcome of the assessment.

    Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

    The estimated completion date is: TBD Pending Confirmation of Funding

    OIG Comment
    OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

32. Establish an integrated AIM and CBTC modernization strategy to prioritize and address technical, operational, infrastructure, data, vendor, and other needs identified through the

readiness and integration assessment to support Red Line CBTC implementation and long-term rail modernization.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 31. Consistent with Strategic Plan Objective 2, the readiness and integration assessment will produce an evidence-based integration and transition strategy that prioritizes technical, operational, infrastructure, data, and vendor needs. The resulting prioritized modernization roadmap will be submitted for approval in Phase 2 (Assess and Design), with approved actions advancing in Phase 4 (Modernize and Integrate).

Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment
OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

33. Establish a vendor-neutral CBTC reference and integration architecture aligned with WMATA's Manual of Design Criteria, applicable requirements, and industry standards to guide system integration, procurement, implementation, and long-term modernization.

Management Response
Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 31. Consistent with Strategic Plan Objective 2 and Objective 3 (Modernize RTUs and Communications Infrastructure), Rail Modernization will establish a vendor-neutral CBTC reference and integration architecture, including the future-state field communications architecture, aligned with WMATA's Manual of Design Criteria, applicable requirements, and industry standards to guide system integration, procurement, implementation, and long-term modernization.

Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

The estimated completion date is: TBD Pending Confirmation of Funding

OIG Comment

OIG considers management's comments responsive to the recommendation and the corrective actions taken should resolve the issue identified in this report. OIG will follow up on the planned actions during the corrective action plan phase.

Scope

The scope of this audit included WMATA's AIM and supporting train control environment, including: (1) strategies and plans for sustaining, modernizing, or replacing the legacy AIM system; (2) risks associated with AIM customization, vendor and key-person dependencies, and system lifecycle management; (3) the condition, reliability, and modernization of aging train control infrastructure, including RTUs and communications; and (4) AIM readiness and integration considerations associated with the planned CBTC modernization. The audit also considered AIM configuration and operational data management, alarm management, cybersecurity, and physical security controls.

The audit covered fiscal years 2022-2026. OIG also considered relevant historical information and events outside this period, as necessary, to understand AIM system performance, operational disruptions, lifecycle conditions, and modernization strategies and decisions.

Methodology

To achieve the audit objective, OIG's audit methodology was as follows:

- Researched and reviewed applicable federal regulations, WMATA requirements, and industry standards and best practices.
- Interviewed personnel from DM, COSI, Power, MICC, the CBTC program, and other responsible organizations to understand AIM operations, governance, maintenance, system support, risks, and modernization activities.
- Reviewed AIM strategies, plans, contracts, system documentation, operational and maintenance records, scan sheets, alarm and historian data, access reports, cybersecurity documentation, and other supporting records.
- Assessed AIM lifecycle and continuity risks.
- Evaluated the condition, reliability, and modernization of RTUs and communications infrastructure, including equipment failures, legacy DTS communications, end-of-life and support conditions, and replacement activities.

- Evaluated AIM configuration data, database integrity, alarm management, cybersecurity, access controls, and physical security, including scan sheet governance, alarm performance, network segmentation, server configurations, vulnerability testing, privileged access, and TCR security.

- Reviewed AIM outages, communications failures, and other performance information to assess impacts on system reliability, MICC operational awareness, continuity, and rail operations.

- Reviewed Red Line CBTC planning and modernization readiness, including AIM and infrastructure dependencies, system interfaces, operational requirements, integration risks, and the need for a vendor-neutral CBTC reference and integration architecture.

- Used applicable FTA requirements and guidance, WMATA criteria, and recognized industry standards and best practices to evaluate audit results and support OIG findings and recommendations.
- Visited WMATA's data centers at Eisenhower that house the AIM systems.

Generally Accepted Government Auditing Standards (GAGAS) Statement

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

ABBREVIATION	DESCRIPTION
ACS	Access Control System
AIM	Advanced Information Management
ANSI/ISA	American National Standards Institute/ International Society of Automation
APTA	American Public Transportation Association
ASV	Approved Scanning Vendor
ATC	Automatic Train Controls
CAP	Corrective Action Plan
CBTC	Communications-Based Train Control
CCTV	Closed-Circuit Television
CFR	Code of Federal Regulations
CIP	Capital Improvement Program
CISA	Cybersecurity & Infrastructure Security Agency
COBIT	Control Objectives for Information Technologies
COSI	Communications and Signaling
DHS	Department of Homeland Security
DM	Digital Modernization
DMA	Direct Memory Access
DNP3	Distributed Network Protocol 3

ABBREVIATION	DESCRIPTION
DOT	Department of Transportation
DTS	Data Transmission System
EEMUA	Engineering Equipment and Materials Users Association
FEP	Front End Processor
FLSZ	Fire/Life-Safety Security Zone
FTA	Federal Transit Administration
ICS/OT	Industrial Control System and Operational Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IIJA	Infrastructure Investment and Jobs Act
KPI	Key Performance Indicator
MICC	Metro Integrated Command Center
MTBF	Mean Time Between Failure
NIST	National Institute of Standards and Technology
OCSZ	Operationally Critical Security Zone
OT	Operational Technology
PIDS	Passenger Information Display System
PLC	Programmable Logic Controller

ABBREVIATION	DESCRIPTION
PSD	Platform Screen Doors
PTASP	Public Transportation Agency Safety Plan
RBAC	Role-Based Access Controls
ROCC	Rail Operations Control Center
RPM	Rail Performance Monitoring
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCSZ	Safety-Critical Security Zone
SQL	Structured Query Language
TAM	Transit Asset Management
TCP	Transmission Control Protocol
TCR	Train Control Room
TPS	Train Progress Server
VBS	Virtualization-Based Security
VLAN	Virtual Local Area Network

The table shows the key operational, infrastructure, communications, data management, and governance deficiencies identified during the audit and their relationship with Red Line CBTC implementation and modernization readiness risks.

CBTC Requirement	Related Audit Finding(s) Identified	Concise Audit Alignment	Risk
High Availability Telemetry and Reliable Field Communications	Aging and Failing RTUs; Legacy DTS Communications; Weak AIM Monitoring and KPI Controls	Aging RTUs and unreliable communications reduce WMATA's ability to maintain accurate visibility into critical rail equipment and operations needed to support safe CBTC operations.	High
Completion of RTU Modernization and DTS to Fiber Upgrade	Aging and Failing RTUs; DTS to Fiber Upgrade Delays; CBTC Readiness Deficiencies	Delays completing RTU modernization and fiber communications upgrades limit infrastructure readiness necessary for Red Line CBTC implementation.	High
Reliable Alarm Management and Minimal False Alarms	Ineffective Alarm Management Controls; Weak Alarm Governance and Lifecycle Management; Weak Root Cause Analysis Practices	Excessive nuisance alarms and weak alarm management reduce operator confidence and increase the risk that critical operational issues may not be identified or addressed timely.	High
Database Integrity and Scan Sheet Reconciliation	Weak Alarm and Scan Sheet Configuration Management; Lack of AIM Data Governance and Baseline Management	Weak database integrity and scan sheet management increase the risk of inaccurate equipment information and unreliable supervisory monitoring.	High
Open Integration Architecture and Reduced Vendor Dependency	Vendor Dependency and Proprietary AIM Environment Risks; Weak AIM Data Governance and Analytics Capabilities	Heavy reliance on proprietary systems increases integration complexity, modernization risk, and long term operational costs.	High
SCADA Lifecycle Management and Total Cost of Ownership (TCO)	Lack of Lifecycle Cost Planning and Vendor Governance; AIM Modernization Deficiencies	WMATA has not fully established long term modernization planning and lifecycle management necessary to support future rail automation efforts.	Medium
Database Precision and Accurate Field Mapping	Weak Scan Sheet Configuration Management; AIM Data Integrity Deficiencies	Inaccurate scan sheet configurations and inconsistent equipment mappings reduce operational visibility and monitoring reliability required for CBTC operations.	High
Integrated Data Management, Historian, and Data Warehouse Capabilities	Lack of AIM Data Governance, Historian, and Analytics Capabilities; CBTC Data Baseline Infrastructure Readiness Gap	WMATA has not established centralized data management and analytics capabilities necessary to support operational reporting, predictive maintenance, and CBTC readiness activities.	High
Modern SCADA and CBTC Subject Matter Expertise and Knowledge Continuity	Key Person Dependency; Limited Modern SCADA and CBTC Expertise; Weak Knowledge Management and Succession Planning	WMATA relies heavily on limited personnel and does not maintain sufficient in-house expertise necessary to support long term SCADA modernization and Red Line CBTC readiness activities.	High

OIG received WMATA's comments on November 6, 2026 (**Appendix E**). WMATA management generally concurred with the findings and recommendations in this report. OIG acknowledges management's statement that AIM was reportedly fully operational 99.9933% of the time during the past year and that WMATA can continue to operate during infrequent AIM interruptions. However, OIG did not independently validate the reported availability metric or management's characterization of operational capabilities during AIM outages as part of this audit. Accordingly, OIG expresses no opinion regarding the accuracy of the reported 99.9933% availability figure or the extent to which rail operations can be sustained during AIM interruptions.

Memorandum

Subject: OIG Audit of WMATA's AIM Supervisory Control and Monitoring of Rail Systems
Date: 11.06.2026

From: Deputy General Manager, Andrew Off
Acting Executive Vice President and Chief Digital Officer, Terrence Goines

To: Inspector General, Michelle Zamarin
CC: GM & CEO – Randy Clarke, SVP & CRAO – Elizabeth Sullivan, Senior Executive Team

WMATA reviewed the Office of Inspector General's (OIG) September 30, 2026, Audit of WMATA's AIM Supervisory Control and Monitoring of Rail Systems (OIG 27-04) and concurs with the audit's overall recommendations and the importance of strengthening governance, documentation, maintenance practices, and management oversight associated with AIM. WMATA's response and accompanying AIM Supervisory Control and Monitoring of Rail Systems Strategic Plan describe the actions underway and planned to address the report's recommendations and strengthen the management of AIM and its supporting infrastructure. Where OIG describes the AIM system as critical to operations, we agree that the AIM system is needed to optimize rail service reliability, efficiency and effectiveness. However, it should be noted that Metro can and does deliver service when AIM is interrupted, on a very infrequent basis. Over the past year, AIM was fully operational 99.9933% of the year.

The OIG report identifies opportunities to strengthen AIM governance, lifecycle management, maintenance, system documentation, and organizational accountability. The AIM Supervisory Control and Monitoring of Rail Systems Strategic Plan addresses these matters through coordinated actions intended to clarify responsibilities, strengthen system management and maintenance practices, improve documentation and oversight, and support the continued reliability and effectiveness of AIM.

Finding 1: DM Has Not Established a Continuity Strategy for the Legacy AIM System

Recommendation:

1. Implement a long-term AIM replacement and continuity strategy that defines the future supervisory control platform, transition approach, key milestones, funding requirements, and contingency plans to maintain uninterrupted rail operations.

   Response: Management concurs. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), the central cross-functional team will first establish an AIM baseline covering performance, capacity, reliability, maintainability, cybersecurity, lifecycle cost, and supportability, and will identify which deficiencies can be corrected through stabilization or optimization. During Phase 2 (Assess and Design), the team will complete an independent AIM feasibility and lifecycle assessment, informed by proportionate market research, peer-transit

consultation, and a workforce assessment, and will compare sustainment, targeted modernization, and replacement options against documented requirements. The resulting options analysis will recommend a future-state course of action and an AIM continuity strategy, including the transition approach, key milestones, funding requirements, and contingency arrangements, for executive approval. The approved course of action will advance in Phase 4 (Modernize and Integrate). Progress will be tracked through the Program Management Office's integrated master schedule and corrective action register, and the analysis will not presume replacement, additional staffing, or a particular supplier.

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

2. Establish software continuity protections by implementing a software escrow agreement and strengthening vendor contracts to provide access to source code, technical documentation, and other critical assets needed to maintain or restore AIM operations if vendor support becomes unavailable.

Response: Management concurs with the need for software continuity protections. Under Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy) and Objective 7 (Reduce Vendor and Key Person Dependency), the central cross-functional team, Procurement, and other internal stakeholders will, during Phase 2 (Assess and Design), assess existing license and contract rights, source-code ownership, third-party dependencies, documentation completeness, and the build and restoration requirements needed to maintain or restore AIM operations if vendor support becomes unavailable. The team will evaluate software escrow or equivalent rights to source materials, technical documentation, recovery assets, and configuration information, including release conditions, deposit verification, update obligations, usability testing, cost, and enforceability. Continuity, documentation, access, performance, and transition requirements will be incorporated into future contracts and task orders. Execution of an escrow agreement will proceed once the assessment supports the arrangement and the required contractual and funding approvals are obtained.

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

3. Conduct an independent engineering and technology feasibility assessment of the AIM platform. Benchmark its performance, capacity, scalability, maintainability, lifecycle costs, and integration capabilities against current industry solutions. Use the results to determine whether AIM remains the most appropriate long-term supervisory control platform or should it be replaced.

Response: An independent engineering and technology assessment of the AIM platform will be completed. The planned Red Line CBTC and central SCADA environment is not intended to connect to or integrate with the existing AIM system. AIM sustainment and modernization for the Blue,

Orange, Silver, Green, and Yellow (BOSGY) lines therefore remain a separate responsibility and investment need. References in this response to coordinated modernization mean coordination of operational readiness, infrastructure dependencies, resource decisions, and transition planning; they do not imply a direct AIM-to-CBTC interface. The absence of that interface does not, by itself, establish that all transition or shared-infrastructure risks have been resolved. Management will document the relevant boundaries and evidence supporting its response to OIG. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), an independent engineering and technology assessment of the AIM platform will be completed in Phase 2 (Assess and Design).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 2: DM Has Not Effectively Managed Vendor and Key-Person Dependencies or Ensured Adequate Contract Oversight
Recommendations:

4. Establish a workforce and operational continuity strategy to reduce key person dependency and strengthen in-house expertise in AIM operations, operational data management, OT communications, and systems integration necessary to support long-term rail modernization.

   Response: Consistent with Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency), Digital Modernization will strengthen the capabilities of the core AIM Support Team (2 Technical Leads, 1 Application Specialist, 1 Developer) so that it can scale to support the system. Management will identify critical roles, competencies, single points of knowledge, and succession risks; develop competency matrices for AIM operations, databases, OT communications, systems integration, cybersecurity, and configuration management; and assign trained primary and backup personnel for critical functions. Structured knowledge transfer, cross-training, and readiness demonstrations will be required, with critical cross-training and knowledge-transfer activities completed in Phase 3 (Implement Priority Controls). Additional positions or training obligations will be proposed only where the workforce assessment demonstrates a need.

   Accountable Organization(s): Digital Modernization – Operations Technology

   The estimated completion date is: TBD Pending Confirmation of Funding

5. Strengthen vendor and contract oversight by enforcing clear responsibilities, validating vendor deliverables and invoices before payment, and implementing performance and cost controls.

   Response: Management concurs with the need to strengthen vendor and contract oversight. Current controls include COTR vendor reviews, delineation of responsibilities between WMATA personnel and contractors, validation of work in lower environments, and approval before

contractor work is implemented in the production environment. Under Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency), management will further clarify WMATA and vendor responsibilities in contracts and task orders and require validation of deliverables, labor hours, materials, and invoices before payment. Existing validation controls continue under Phase 1 (Mobilize and Stabilize), and contract oversight and cost recovery procedures will be strengthened in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

6. Strengthen project management governance and oversight by implementing centralized coordination, reconciliation, and labor hour validation controls to prevent duplicative work and unnecessary payments.

Response: Management concurs. Under Strategic Plan Objective 1 (Establish Executive Governance and Accountability), the Program Management Office will provide centralized coordination of AIM-related work through the integrated master schedule, decision log, dependency map, and corrective action register so that overlapping or duplicative activities are identified before work is authorized. Under Objective 4 (Strengthen Configuration and Change Management), project deliverables, database changes, labor hours, and field implementation records will be reconciled before payment approval. These controls build on existing COTR vendor reviews, delineation of WMATA and contractor responsibilities, lower-environment validation, and production approval. Validation controls continue under Phase 1 (Mobilize and Stabilize) and will be strengthened in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 3: WMATA Relies on Outdated RTUs and Legacy Communications Infrastructure

Recommendations:

7. Implement a comprehensive RTU modernization strategy that accelerates replacement of aging RTUs, prioritizes upgrades based on asset condition, failure history, operational criticality, and lifecycle risk, and improves system reliability through enhanced visibility and automation.

Response: The central cross-functional team will coordinate an Infrastructure-led assessment of RTU inventory and condition, failure history, communications coverage, operational criticality, supportability, security capabilities, integration constraints, and existing approved project scope. Market research will compare feasible equipment and communications options, lifecycle support, interoperability, installation requirements, maintenance skills, and total ownership cost. Peer-transit consultation will examine migration sequencing, testing, outage management, and lessons

from legacy field-equipment modernization. Engineering and safety review will determine where laboratory validation or a controlled field pilot is needed before scaling. The team will recommend a prioritized and costed stabilization and modernization roadmap, with scope and acceleration decisions reserved for the required approvals.

Accountable Organization(s): Infrastructure – Communications & Signaling, Digital Modernization – Operational Technology

The estimated completion date is: TBD Pending Confirmation of Funding

8. Implement controls to clearly identify, track, and report RTU upgrade costs within the TCR Renewal Project budget and strengthen budget governance through complete expenditure documentation and dedicated RTU line-item reporting.

   Response: The actions necessary to address this recommendation are encompassed within the corrective actions established for Recommendation 7. Accordingly, these actions will be implemented and tracked through the same coordinated approach to avoid duplicative efforts. This aligns with Strategic Plan Objective 3, which provides for evaluating dedicated RTU budget line items and expenditure controls and for separately tracking and reconciling RTU expenditures.

   Accountable Organization(s): Infrastructure – Communications & Signaling

   The estimated completion date is: TBD Pending Confirmation of Funding

9. Accelerate completion of the DTS-to-Fiber Upgrade Project by prioritizing fiber connectivity to high-risk and critical rail locations and aligning RTU modernization efforts to restore system visibility, reduce dark territory conditions, improve operational reliability, and support the successful implementation of the Red Line CBTC program.

   Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 7 to avoid duplicative effort. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure), RTU replacement will be coordinated with the DTS-to-Fiber Upgrade Project, and fiber connectivity will be prioritized for critical and high-risk rail locations to restore system visibility and reduce dark territory conditions. Priority locations will be identified in Phase 1 (Mobilize and Stabilize), initial fiber priorities will be executed in Phase 3 (Implement Priority Controls), and modernization will expand in Phase 4 (Modernize and Integrate). Coordination with Rail Modernization will address shared infrastructure and transition dependencies relevant to the Red Line CBTC program.

   Accountable Organization(s): Infrastructure – Communications & Signaling, Rail Modernization, Digital Modernization – Operational Technology

   The estimated completion date is: TBD Pending Confirmation of Funding

Finding 4: WMATA Does Not Effectively Manage Critical AIM Configuration Settings
Recommendations:

10. Establish a centralized AIM scan sheet configuration and database integrity program that requires that (a) scan sheet changes be reviewed, validated, reconciled with field equipment, formally approved through a change control board, and (b) scan sheets be periodically monitored to ensure configuration accuracy, integrity, and reliability.

    Response: Management concurs. Consistent with Strategic Plan Objective 4 (Strengthen Configuration and Change Management), Digital Modernization will serve as technical owner of a centralized AIM configuration management program and authoritative repository for all scan sheets and configuration records, with ATC, SCADA Engineering, and Ventilation accountable for review and validation within their operational domains. Undocumented production changes, except emergency actions, will be frozen in Phase 1 (Mobilize and Stabilize); configuration standards, decision rights, and escalation procedures will be established in Phase 2 (Assess and Design); and the centralized repository, baseline controls, and Change Control Board (CCB) governance will be implemented in Phase 3 (Implement Priority Controls). Configuration changes will require independent review, field reconciliation, testing, documented validation, and CCB approval before production implementation, and scan sheets will be periodically audited and recertified.

    Accountable Organization(s): Digital Modernization – Operations Technology

    The estimated completion date is: TBD Pending Confirmation of Funding

11. Strengthen project coordination and accountability controls to prevent duplicate or conflicting scan sheet configurations and ensure AIM modernization activities, labor hours, and database changes are properly reconciled, validated, and aligned with approved project and contractual requirements.

    Response: Management concurs. Consistent with Strategic Plan Objective 1 (Establish Executive Governance and Accountability) and Objective 4 (Strengthen Configuration and Change Management), Digital Modernization will implement project governance controls, coordinated through the Program Management Office, that require departments, project teams, and contractors to reconcile scan sheet changes, labor hours, project deliverables, and database modifications before implementation and payment approval. Management will maintain configuration baselines, track approved changes through the decision log and dependency map, validate implementation results, and conduct periodic configuration audits and recertifications to identify and resolve duplicate, conflicting, or unauthorized configurations. These controls will be implemented in Phase 3 (Implement Priority Controls).

    Accountable Organization(s): Digital Modernization – Operations Technology

    The estimated completion date is: TBD Pending Confirmation of Funding

12. Document AIM scan sheet governance, validation, reconciliation, and configuration management activities within WMATA's PTASP and Safety Risk Management processes and establish appropriate controls to monitor and mitigate associated operational risks.

    Response: Management concurs. Consistent with Strategic Plan Objective 4 (Strengthen Configuration and Change Management) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Safety will incorporate AIM scan sheet governance, validation, reconciliation, and configuration management activities into WMATA's PTASP, Safety Risk Management, and Management of Change processes. Configuration changes that may affect supervisory monitoring, alarm functionality, equipment status, or operational control will require a documented safety risk assessment before deployment. Safety will document mitigation requirements, approval authorities, validation procedures, and ongoing monitoring, with Digital Modernization supporting as technical owner. Success will be measured by safety-significant configuration changes receiving documented risk review before deployment.

    Accountable Organization(s): Safety and Readiness – Safety (Lead), Digital Modernization as technical owner

    The estimated completion date is: TBD Pending Confirmation of Funding

Finding 5: WMATA Lacks Effective AIM Operational Data Governance and Management
Recommendations:

13. Establish a formal AIM operational data governance and database integrity program with defined roles and responsibilities, standardized procedures, documented knowledge transfer and cross-training, and controls for backup, synchronization, reconciliation, historical data management, and operational baseline management.

    Response: Management concurs. Under Strategic Plan Objective 5 (AIM operational data governance and management), existing backups will be validated and a priority restoration test performed in Phase 1 (Mobilize and Stabilize), and the daily database backups, hourly transaction log backups, and twice-daily historian archives will be evaluated based on recoverability evidence. In Phase 2 (Assess and Design), the central cross-functional team will complete a data assessment and establish governance standards defining data ownership and stewardship, standardized procedures, synchronization and reconciliation controls, retention and historical data management, operational baseline management, and documented knowledge transfer and cross-training. Success will be measured by successful backup and restoration testing and by the assignment of an owner and steward to each critical dataset.

    Accountable Organization(s): Digital Modernization – Operations Technology

    The estimated completion date is: TBD Pending Confirmation of Funding

14. Implement a centralized AIM data management platform that has the ability to consolidate operational and historical data and support standardized reporting and analytics, KPI monitoring of system performance and reliability, and predictive analysis to improve operational and maintenance decision-making and Red Line CBTC readiness.

Response: Management concurs with the need for improved reporting, KPI monitoring, and analytics. These actions will be implemented and tracked with the corrective actions for Recommendation 13. Consistent with Strategic Plan Objective 5, operational and maintenance stakeholders will define reporting use cases, KPI definitions, and predictive-analysis needs during Phase 2 (Assess and Design), and market research and peer-transit benchmarking will compare enhancing existing tools with adding a centralized platform. Any approved centralized AIM data management and analytics capability will be implemented in Phase 4 (Modernize and Integrate), subject to the approved assessment and business case, with AIM/BOSGY and Red Line needs assessed separately.

Accountable Organization(s): Rail Modernization, Digital Modernization – Operations Technology

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 6: WMATA Lacks Effective AIM Alarm Management, Root Cause Analysis, and System Performance Monitoring

Recommendations:

15. Establish a formal AIM alarm management process with designated personnel, roles, and responsibilities to improve alarm design and control, including alarm governance, rationalization, prioritization, threshold management, and suppression and partitioning controls.

Response: Management concurs. Consistent with Strategic Plan Objective 6 (Improve Alarm Management, Reliability, and Root Cause Analysis), MICC and technical domain owners, coordinated through the central cross-functional team, will establish an AIM alarm management philosophy and governance standard in Phase 2 (Assess and Design) that designates personnel, roles, and responsibilities and defines alarm rationalization, prioritization, threshold management, and suppression and partitioning controls. The assessment will address alarm inventory, nuisance and recurring conditions, operator workload, response procedures, and escalation criteria, informed by peer-transit practices. Engineering and Safety will review operational consequences and define testing, approval, rollback, and monitoring requirements; changes will not be justified solely by reducing alarm volume. Priority alarm rationalization will be implemented in Phase 3 (Implement Priority Controls), and alarm performance will be continuously improved in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

16. Perform a comprehensive review and rationalization of AIM alarms to identify, correct, and monitor nuisance and excessive alarm conditions affecting AIM reliability and operational awareness.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15. Consistent with Strategic Plan Objective 6, a comprehensive alarm rationalization will identify and correct chattering, fleeting, stale, duplicate, and recurring alarms, with priority rationalization completed in Phase 3 (Implement Priority Controls). Results will be monitored through the Strategic Plan's Performance Dashboard, including alarm volume, nuisance-alarm percentage, and repeat alarms, and improved continuously in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

17. Implement appropriate access restrictions and monitoring controls over AIM alarm inhibition, override, partitioning, and suppression functions to ensure these functions are used only by authorized personnel.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15 and the access control actions for Recommendation 25. Consistent with Strategic Plan Objective 6 and Objective 8 (Strengthen Cybersecurity and Access Controls), AIM alarm inhibition, override, partitioning, and suppression functions will be restricted to authorized roles, privileged alarm actions will be centrally logged, and those logs will be periodically reviewed. These controls will be implemented in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling, Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

18. Establish a formal AIM root cause analysis process with defined escalation criteria, cross-functional coordination among DM, COSI, Power, MICC, and other responsible stakeholders, centralized tracking, and corrective action accountability to identify and resolve underlying causes and prevent recurring AIM operational problems.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 15. Consistent with Strategic Plan Objective 6, RCA standards will be established in Phase 2 (Assess and Design), defining escalation thresholds for

significant outages, communications failures, alarm floods, and recurring events and assigning cross-functional responsibilities among DM, COSI, Power, MICC, and other responsible stakeholders. Centralized RCA and corrective action tracking will be implemented in Phase 3 (Implement Priority Controls), with corrective actions tracked through verified closure and reported through the Performance Dashboard's RCA completion and corrective action closure measures.

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications and Signaling (COSI), Operations – Metro Integrated Command & Communications Center

The estimated completion date is: TBD Pending Confirmation of Funding

19. Establish a formal AIM performance monitoring and reporting program with standardized performance measures, KPIs, and routine management reporting to monitor alarm performance, AIM reliability, and RTU and field equipment performance and health.

Response: Management concurs. Consistent with Strategic Plan Objective 6 and the Strategic Plan's Performance Dashboard, Digital Modernization will establish an AIM performance monitoring and reporting program that defines performance measures, KPI thresholds, reporting responsibilities, and governance requirements. KPI baselines and executive dashboards will be established in Phase 2 (Assess and Design) and will cover AIM availability and major outage trends; RTU availability, failure rate, and replacement progress; alarm volume, nuisance-alarm percentage, and repeat alarms; and RCA completion and corrective action closure. Routine management reporting will use these results to prioritize corrective actions, modernization investments, and reliability improvements.

Accountable Organization(s): Digital Modernization – Operations Technology, Infrastructure – Communications & Signaling, Infrastructure – Power, Infrastructure – Facilities, Metro Integrated Command Center

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 7: Physical Access Controls to Critical Train Control Rooms Need Strengthening

Recommendation(s):

20. Conduct a cost/benefit analysis and risk assessment to determine the sufficiency of current security and access controls for TCRs. Based on that analysis, implement additional security and access controls, such as badge access readers and electronic access logging.

Response: Management concurs. Consistent with Strategic Plan Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Communications and Signaling, in coordination with the Metro Transit Police Department, Digital Modernization, and operating departments, will complete a risk

assessment and cost-benefit analysis of Train Control Room (TCR) physical security controls in Phase 2 (Assess and Design), evaluating key management, access authorization, access monitoring, and surveillance coverage. Based on the results, risk-prioritized enhancements, such as electronic badge access, automated access logging, key inventory and reconciliation, and CCTV monitoring, will be implemented at priority locations in Phase 3 (Implement Priority Controls), with broader physical security improvements completed in Phase 4 (Modernize and Integrate). Periodic reviews of TCR access records and security controls will be established to sustain accountability.

Accountable Organization(s): Communications and Signaling (COSI), Digital Modernization, and MTPD support

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 8: Cybersecurity Controls Over AIM and Interfaced Train Control Systems Need Strengthening

Recommendations:

21. Update and maintain a current AIM cybersecurity governance program aligned with industry best practices such as NIST Special Publication 800-82 Revision 3, including defined security policies, standards, risk assessments, responsibilities, and monitoring requirements to support secure and reliable AIM operations.

    Response: Management concurs. Consistent with Strategic Plan Objective 8 (Strengthen Cybersecurity and Access Controls), Digital Modernization – Cybersecurity will update and maintain an AIM cybersecurity governance program defining security policies, standards, risk assessment requirements, responsibilities, and monitoring requirements. Privileged and vendor access reviews will begin in Phase 1 (Mobilize and Stabilize). In Phase 2 (Assess and Design), the central cross-functional team and Cybersecurity will complete a cybersecurity assessment of control coverage, asset and network visibility, security boundaries, privileged and vendor access, server configuration, and legacy constraints, supported by a standards-applicability register referencing NIST SP 800-82 Revision 3, applicable CIS Windows Server guidance, and relevant APTA publications. AIM will continue to be managed as a subsystem within the DM OT Boundary in Archer, with associated risks documented in the Risk Register. Enhanced controls will be deployed in Phase 3 (Implement Priority Controls) following compatibility assessment, safety and reliability review, testing, rollback planning, and approval.

    Accountable Organization(s): Digital Modernization - Cybersecurity

    The estimated completion date is: TBD Pending Confirmation of Funding

22. [redacted]

Response: Management concurs. These actions will be implemented and tracked with the [redacted]

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: TBD Pending Confirmation of Funding

23. Modernize and secure legacy RTUs and communications supporting AIM through phased replacement and implementation of appropriate authentication, encryption, integrity protections, and other OT cybersecurity controls consistent with NIST guidance.

Response: Management concurs. These actions will be implemented through the RTU and communications modernization roadmap established for Recommendation 7. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure) and Objective 8 (Strengthen Cybersecurity and Access Controls), authentication, integrity, encryption, and logging controls will be incorporated into RTU and communications modernization where technically feasible, and cybersecurity testing will be required before operational acceptance. Implementation will follow the RTU and fiber sequence in Phase 3 (Implement Priority Controls) and Phase 4 (Modernize and Integrate), led by Infrastructure – Communications and Signaling in coordination with Digital Modernization.

Accountable Organization(s): Infrastructure - Communications and Signaling

The estimated completion date is: TBD Pending Confirmation of Funding

24. Strengthen AIM cybersecurity by establishing and documenting defined security zones, effective network segmentation, layered security controls, and routine firewall rule reviews consistent with APTA and NIST guidance.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8, Cybersecurity will define and document AIM security zones, segmentation requirements, approved communications paths, layered security controls, and firewall governance, informed by APTA and [redacted]

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: 12/31/2028

25. Strengthen AIM access controls by implementing role-based and privileged access management, separating development, test, and production environments, periodically reviewing user access, and restricting vendor access to critical operational systems.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8, Cybersecurity will implement role-based and privileged access controls based on least-privilege principles, separate development, test, and production environments, perform periodic user access reviews, and restrict and monitor vendor access to critical operational systems. Privileged and vendor access reviews will begin in Phase 1 (Mobilize and Stabilize), and enhanced access and privileged access controls will be deployed in Phase 3 (Implement Priority Controls).

Accountable Organization(s): Digital Modernization – Cybersecurity

The estimated completion date is: 09/30/2027

Finding 9: WMATA Lacks Integrated Risk Management Over the AIM System

Recommendations:

26. Establish a formal AIM operational risk assessment process aligned with best practices, with defined ownership, periodic risk reviews, mitigation tracking, and ongoing monitoring to ensure risks that affect AIM system reliability and rail operations are consistently identified, prioritized, and addressed.

Response: Management concurs. DM Cybersecurity Services (DMCS) has established a formal cybersecurity risk management framework in which AIM is identified as a subsystem within the DM OT Boundary in Archer, and AIM cybersecurity and operational risks are documented, assessed, tracked, and monitored in the Risk Register and linked to Key Risk Indicators (KRIs), Key Control Indicators (KCIs), mitigation activities, and Plans of Action and Milestones (POA&Ms). Consistent with Strategic Plan Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), these AIM risks will be linked to the Strategic Plan's consolidated risk register, which defines risk scoring, acceptance authorities, mitigation requirements, and review frequency and connects operational and cybersecurity risks to corrective actions and investment decisions. DMCS will perform periodic AIM risk assessments and reviews, monitor mitigation through completion, and maintain current risk ratings, owners, target dates, and status. Success will be measured by all high and critical risks having approved treatments and owners and by risk reviews completed on schedule.

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: 06/30/2027

27. Establish a formal AIM lifecycle, vendor dependency, and knowledge management risk assessment process to identify and address replacement needs, asset sustainability, vendor reliance, knowledge transfer, and workforce readiness needed to support reliable operations and future rail modernization.

Response: Management concurs. Consistent with Strategic Plan Objective 7 (Reduce Vendor and Key Person Dependency) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Digital Modernization, in coordination with Cybersecurity, will implement a recurring lifecycle, vendor dependency, and workforce readiness risk assessment for the AIM environment, evaluating asset supportability, technology obsolescence, vendor reliance, workforce capabilities, succession risks, knowledge-transfer requirements, and related cybersecurity risks. Identified risks will be recorded in the consolidated risk register with owners and treatments, and results will inform modernization, continuity, cybersecurity, workforce, and investment decisions through the annual strategy, lifecycle, risk, workforce, and architecture reviews conducted in Phase 5 (Sustain and Optimize).

Accountable Organization(s): Digital Modernization

The estimated completion date is: TBD Pending Confirmation of Funding

28. Establish a formal AIM data governance, data quality, and integrity risk assessment process to identify and address risks related to data architecture, system integrity, analytics capabilities, workforce skills, and technology needs that could affect operational reliability and future modernization, including the Red Line CBTC program.

Response: Management concurs. Consistent with Strategic Plan Objective 5 (AIM operational data governance and management) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Digital Modernization, in coordination with Cybersecurity and Rail Modernization, will establish a periodic AIM data governance and data integrity risk assessment covering data quality, database integrity, configuration accuracy, data architecture, analytics capabilities, workforce competencies, and supporting technologies. Identified risks will be recorded in the consolidated risk register with documented mitigation plans and accountable owners. Rail Modernization will provide input on modernization priorities, integration requirements, lifecycle planning, and future-state operational needs, and, consistent with Objective 2, Red Line CBTC considerations will be addressed through validation of CBTC/SCADA scope, dependencies, and AIM/BOSGY requirements.

Accountable Organization(s): Digital Modernization – Operational Technology, Rail Modernization

The estimated completion date is: TBD Pending Confirmation of Funding

29. Establish a comprehensive risk assessment for AIM RTUs and supporting communications infrastructure, identify and address lifecycle and integration risks, define the future-state architecture, and support reliable operations and future rail modernization.

Response: Management concurs. These actions will be implemented and tracked with the RTU and communications corrective actions for Recommendations 7 and 23. Consistent with Strategic Plan Objective 3 (Modernize RTUs and Communications Infrastructure) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), Infrastructure – Communications and Signaling will complete RTU and communications risk assessments in Phase 2 (Assess and Design) to identify lifecycle and integration risks and will define a vendor-neutral future-state field communications architecture. Identified risks will be recorded in the consolidated risk register and linked to the prioritized RTU and fiber modernization roadmap.

Accountable Organization(s): Infrastructure - Communications and Signaling

The estimated completion date is: TBD Pending Confirmation of Funding

30. Establish a comprehensive AIM cybersecurity risk assessment process to identify and address operational technology risks related to defense-in-depth, access controls, vendor dependencies, software security, and legacy technologies that could affect secure and reliable rail operations and future modernization.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 21. Consistent with Strategic Plan Objective 8 (Strengthen Cybersecurity and Access Controls) and Objective 9 (Integrate Enterprise Risk, Safety, and Physical Security), the AIM cybersecurity assessment completed in Phase 2 (Assess and Design) will address defense-in-depth, access controls, vendor dependencies, software security, and legacy technology risks. Results will be documented in the Archer Risk Register, linked to the consolidated risk register, and tied to corrective actions and investment decisions, with periodic reassessments to keep the risk profile current.

Accountable Organization(s): Digital Modernization - Cybersecurity

The estimated completion date is: TBD Pending Confirmation of Funding

Finding 10: Red Line CBTC Migration Readiness is Limited by AIM Technical Deficiencies and the Lack of a Vendor-Neutral CBTC Reference and Integration Architecture

Recommendations:

31. Conduct a formal CBTC modernization readiness and integration assessment to evaluate AIM technical debt, infrastructure dependencies, system interfaces, operational requirements, vendor and workforce dependencies, and other factors that could affect the transition to Red Line CBTC.

Response: Management concurs. Consistent with Strategic Plan Objective 2 (Define the AIM Future State and Continuity Strategy), Rail Modernization, supported by Digital Modernization – Operational Technology and coordinated through the central cross-functional team, will conduct a CBTC readiness and integration assessment in Phase 2 (Assess and Design). The assessment will validate Red Line CBTC/SCADA boundaries, required supervisory functions, field and communications dependencies, operational transition requirements, cybersecurity responsibilities, vendor and workforce dependencies, and the continuing AIM/BOSGY scope. It will document which AIM risks have no direct Red Line interface dependency, which affect continuing operations, and which shared or transition dependencies require action. Vendor-neutral market research and peer-transit consultation will inform requirements and acceptance criteria, and proposals will be reviewed against WMATA's Manual of Design Criteria and applicable industry requirements. The planned 2034 milestone and proposed procurement will not predetermine the outcome of the assessment.

Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

The estimated completion date is: TBD Pending Confirmation of Funding

32. Establish an integrated AIM and CBTC modernization strategy to prioritize and address technical, operational, infrastructure, data, vendor, and other needs identified through the readiness and integration assessment to support Red Line CBTC implementation and long-term rail modernization.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 31. Consistent with Strategic Plan Objective 2, the readiness and integration assessment will produce an evidence-based integration and transition strategy that prioritizes technical, operational, infrastructure, data, and vendor needs. The resulting prioritized modernization roadmap will be submitted for approval in Phase 2 (Assess and Design), with approved actions advancing in Phase 4 (Modernize and Integrate).

Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

The estimated completion date is: TBD Pending Confirmation of Funding

33. Establish a vendor-neutral CBTC reference and integration architecture aligned with WMATA's Manual of Design Criteria, applicable requirements, and industry standards to guide system integration, procurement, implementation, and long-term modernization.

Response: Management concurs. These actions will be implemented and tracked with the corrective actions for Recommendation 31. Consistent with Strategic Plan Objective 2 and Objective 3 (Modernize RTUs and Communications Infrastructure), Rail Modernization will establish a vendor-neutral CBTC reference and integration architecture, including the future-state field communications architecture, aligned with WMATA's Manual of Design Criteria, applicable requirements, and industry standards to guide system integration, procurement, implementation, and long-term modernization.

Accountable Organization(s): Rail Modernization (Lead), Digital Modernization – Operational Technology (Support)

The estimated completion date is: TBD Pending Confirmation of Funding

Strategic Plan in Response to the OIG Audit of AIM Supervisory Control and Monitoring of Rail Systems

1. Purpose

This strategic plan establishes a coordinated, risk-based response to the OIG audit findings concerning the AIM supervisory control environment. It provides the governance, priorities, initiatives, accountability measures, and implementation framework necessary to:

- Sustain safe and reliable rail operations.
- Reduce operational, technology, cybersecurity, vendor, and workforce risks.
- Modernize aging AIM, RTU, and communications infrastructure.
- Strengthen management controls and accountability.

2. Strategic Vision

WMATA will establish a secure, resilient, supportable, and data-driven supervisory control environment that maintains uninterrupted rail operations

3. Guiding Principles

1. Safety and operational continuity first.
2. Risk-based investment and prioritization.
3. Clear accountability across organizational boundaries.
4. Vendor independence and internal capability development.
5. Cybersecurity by design and defense in depth.
6. Authoritative data, controlled configurations, and documented decisions.
7. Measurable results are supported by transparent reporting.

4. Strategic Objectives

Objective 1 — Establish Executive Governance and Accountability

Create an executive-level AIM Optimization and Stabilization central cross-function team chaired by Digital Modernization and supported by Infrastructure, Rail Modernization, Safety, Operations, Cybersecurity, Finance, Procurement, Legal, Communications & Signaling (COSI), MTPD, and MICC leadership.

Key actions:

- Assign an executive sponsor and a single accountable program executive.
- Establish workstream leads for each strategic objective.
- Create a Risk Register covering all 33 recommendations.
- Approve scope, ownership, milestones, funding, dependencies, and closure evidence.
- Conduct monthly program reviews and quarterly executive briefings.

- Establish an escalation process for schedule, funding, safety, or operational risks.
- Require independent validation before recommendations are submitted for closure.

Success measures:

- Every recommendation has an accountable executive, action owner, due date, and closure criteria.
- No overdue high-risk action remains without an approved recovery plan.
- Quarterly status reports reconcile progress, expenditures, risks, and supporting evidence.

Objective 2 — Define the AIM Future State and Continuity Strategy

Develop a long-term supervisory control strategy that determines whether AIM should be sustained, modernized, incrementally replaced, or transitioned to a successor platform.

Key actions:

- Commission an independent engineering and technology assessment.
- Evaluate reliability, capacity, scalability, maintainability, cybersecurity, interoperability, lifecycle cost, and vendor supportability.
- Define the future-state supervisory control architecture.
- Establish transition phases, funding requirements, contingency arrangements, and decision gates.
- Recommend a continuity-of-operations plan covering platform failure, vendor withdrawal, staffing loss, data restoration, and major communications outages.
- Evaluate software escrow or equivalent rights to source materials, technical documentation, recovery assets, and configuration information.
- Align AIM decisions with capital planning, asset management, BOSGY requirements.
- Validate CBTC/SCADA scope, dependencies, and AIM/BOSGY requirements to develop an evidence-based integration and transition strategy.

Success measures:

- Independent assessment completed and accepted.
- Preferred future-state solution approved by executive leadership.
- Funded multiyear roadmap incorporated into the capital program.
- Continuity strategy tested through documented exercises.

Objective 3 — Modernize RTUs and Communications Infrastructure

Implement a coordinated, risk-based program to replace obsolete RTUs and accelerate fiber connectivity.

Key actions:

- Establish a complete inventory of RTUs, communications paths, software versions,

support status, failure history, and criticality.

- Develop a prioritization model based on asset condition, operational consequences, dark territory exposure, cybersecurity risk, and SCADA dependency.
- Coordinate RTU replacement with the DTS-to-Fiber program.
- Prioritize critical and high-risk rail locations.
- Define a vendor-neutral future-state field communications architecture.
- Evaluate/recommend dedicated RTU budget line items and expenditure controls.
- Require commissioning, failover, performance, and cybersecurity testing before operational acceptance.

Success measures:

- Percentage of obsolete RTUs replaced.
- Percentage of priority locations migrated to fiber.
- Reduction in dark territory events and communications failures.
- Improved RTU availability and restoration time.
- RTU expenditures are separately tracked and reconciled.

Objective 4 — Strengthen Configuration and Change Management

Establish one authoritative configuration management program for AIM scan sheets, databases, field equipment, interfaces, and alarm settings.

Key actions:

- Create a centralized repository for approved scan sheets and configuration records.
- Define naming, versioning, approval, retention, and access standards.
- Require independent technical review, field reconciliation, testing, validation, and Change Control Board approval.
- Maintain configuration baselines for development, testing, and production environments.
- Reconcile project deliverables, database changes, labor hours, and field implementation records.
- Conduct periodic configuration audits and recertifications.
- Integrate safety-impacting changes with Safety Risk Management and Management of Change processes.

Success measures:

- All production changes traceable to approved change records.
- Percentage of scan sheets reconciled with field conditions.
- Reduction in unauthorized, duplicate, or conflicting configurations.
- Closure of configuration discrepancies within established service targets.

Objective 5 — Establish Operational Data Governance and Analytics

Create an authoritative, controlled, and recoverable AIM operational data environment.

Key actions:

- Assign data owners and stewards for operational, configuration, alarm, historian, asset, and performance data.
- Standardize backup, recovery, synchronization, reconciliation, archival, retention, and baseline procedures.
- Validate daily database backups, hourly transaction log backups, and twice-daily historian archives.
- Conduct scheduled recovery testing.
- Evaluate and implement a centralized AIM data management platform for the BOSGY lines while coordinating with the future Red Line SCADA environment.
- Develop standardized dashboards for reliability, alarms, RTU health, communications status, outages, and corrective actions.
- Implement data quality rules and periodic integrity assessments.

Success measures:

- Successful backup and restoration testing.
- Percentage of critical datasets assigned to an owner and steward.
- Reduction in reconciliation and data-quality exceptions.
- Availability of standardized operational and executive KPI reporting.
- Predictive maintenance use cases placed into operation.

Objective 6 — Improve Alarm Management, Reliability, and Root Cause Analysis:
Implement formal processes to reduce nuisance alarms, improve operational awareness, and eliminate recurring failures.

Key actions:

- Establish an AIM alarm management philosophy and governance standard.
- Define alarm priorities, thresholds, suppression rules, partitioning authority, and approval requirements.
- Perform a comprehensive alarm rationalization effort.
- Identify and correct chattering, fleeting, stale, duplicate, and recurring alarms.
- Restrict alarm inhibition, override, partitioning, and suppression functions to authorized roles.
- Establish centralized logging and periodic review of privileged alarm actions.
- Define RCA escalation thresholds for significant outages, communications failures, alarm floods, and recurring events.
- Track corrective actions through verified closure.

Success measures:

- Reduction in nuisance and recurring alarms.
- Improved actionable-alarm ratio.
- Percentage of qualifying incidents receiving timely RCA.
- Corrective action closure rate.
- Improvements in system availability, mean time to repair, and recurrence rate.

Objective 7 – Reduce Vendor and Key Person Dependency

Build sustainable internal capability and strengthen vendor accountability.

Key actions:

- Identify critical roles, competencies, single points of knowledge, and succession risks.
- Develop competency matrices for AIM operations, databases, OT communications, systems integration, cybersecurity, and configuration management.
- Assign trained primary and backup personnel for critical functions.
- Require structured knowledge transfer, cross-training, and readiness demonstrations.
- Centralize technical documentation and operating procedures.
- Clarify WMATA and vendor responsibilities in contracts and task orders.
- Validate deliverables, labor hours, materials, and invoices before payment.
- Investigate and recover unsupported, duplicate, or erroneous charges.
- Include continuity, documentation, access, performance, and transition requirements in future contracts.

Success measures:

- Critical functions have qualified backup coverage.
- Knowledge-transfer plans completed and tested.
- Reduction in sole-source or key-person operational dependencies.
- Percentage of vendor deliverables accepted using documented criteria.
- Unsupported costs identified and recovered.

Objective 8 — Strengthen Cybersecurity and Access Controls

Implement a defense-in-depth cybersecurity program for AIM and connected train control systems.

Key actions:

- Maintain an AIM-specific cybersecurity governance and risk management plan.
- Maintain a risk register with risks, KRIs, KCIs, deficiencies, POA&Ms, owners, and target dates.
- Establish approved secure baselines for AIM Windows servers and supporting infrastructure.
- Implement system hardening, encryption, vulnerability remediation, monitoring, and compliance validation.
- Define security zones, segmentation requirements, approved communications paths, and firewall governance.
- Conduct periodic firewall rules and segmentation reviews.
- Implement role-based and privileged access controls using least-privilege principles.
- Separate development, testing, and production environments.

- Restrict and monitor vendor access.
- Incorporate authentication, integrity, encryption, and logging controls into RTU and communications modernization where technically feasible.

Success measures:

- Percentage of systems compliant with approved baselines.
- Reduction in overdue critical vulnerabilities and POA&Ms.
- Completion rate for access recertifications.
- Percentage of privileged and vendor activity logged and reviewed.
- Closure of unauthorized pathways and excessive firewall rules.

Objective 9 — Integrate Enterprise Risk, Safety, and Physical Security

Establish a unified process for managing operational, lifecycle, cybersecurity, data, vendor, workforce, safety, and physical security risks.

Key actions:

- Maintain a consolidated risk register.
- Define risk scoring, acceptance authorities, mitigation requirements, and review frequency.
- Link operational and cybersecurity risks to corrective actions and investment decisions.
- Conduct periodic lifecycle, vendor dependency, workforce readiness, data integrity, RTU, communications,.
- Complete a cost-benefit and risk assessment of Train Control Room physical security.
- Prioritize badge access, electronic logging, key control, surveillance, and periodic access reviews based on risk.
- Integrate relevant AIM risks and controls into PTASP and Safety Risk Management processes.

Success measures:

- All high and critical risks have approved treatments and owners.
- Risk reviews completed according to schedule.
- Physical security improvements implemented at priority locations.
- Safety-significant configuration changes receive documented risk review before deployment.

5. Phased Implementation Roadmap

Phase 1 — Mobilize and Stabilize: TBD Pending Confirmation of funding

- Appoint the executive sponsor, program executive, workstream leads, and action owners.
- Establish the Central cross-functional team and Program Management Office.
- Create the integrated action, risk, dependency, and evidence registers.
- Define closure criteria for all recommendations.

- Identify immediate operational, cybersecurity, configuration, vendor, and continuity risks.
- Freeze undocumented production changes except for emergency actions.
- Validate backups and perform a priority restoration test.
- Begin privileged access and vendor access reviews.
- Continue invoice, labor-hour, and deliverable validation controls.
- Identify high-risk RTUs, dark territory locations, and critical communications gaps.
- Define near-term funding and procurement requirements.

Phase 2 — Assess and Design: TBD Pending Confirmation of funding

- Complete independent AIM feasibility and lifecycle assessment.
- Develop the AIM continuity and future-state strategy.
- Research AIM sustainment, modernization, and successor-platform options for lifecycle cost, interoperability, cybersecurity, and vendor support.
- Benchmark peer-transit architecture, reliability, governance, continuity, and vendor support to inform the future-state strategy and modernization roadmap.
- Complete RTU, fiber, configuration, data, cybersecurity, workforce, and physical access assessments.
- Establish alarm management, RCA, configuration, data governance, and risk management standards.
- Establish a current-state baseline, stabilization exit criteria for reliability, recovery, configuration control, and risk reduction, and optimization targets for alarms, restoration time, analytics, and predictive maintenance; obtain executive approval before implementation.
- Approve the prioritized modernization roadmap, funding strategy, and target milestones.
- Establish KPI baselines and executive dashboards.

Phase 3 — Implement Priority Controls: TBD Pending Confirmation of funding

- Implement centralized repositories, baseline controls, and change governance.
- Complete priority alarm rationalization.
- Deploy enhanced access, privileged access, monitoring, segmentation, and server hardening controls.
- Execute initial RTU replacement and fiber priorities.
- Complete critical cross-training and knowledge-transfer activities.
- Perform initial Train Control Room security upgrades.
- Implement centralized RCA and corrective action tracking.
- Strengthen contract oversight and cost recovery procedures.

Phase 4 — Modernize and Integrate: TBD Pending Confirmation of funding

- Expand RTU and fiber modernization.
- Implement centralized AIM data management and analytics capabilities.
- Advance AIM platform modernization or successor-platform transition.
- Complete broader physical security improvements.
- Verify that workforce, vendor, continuity, and recovery arrangements support the future state.

Phase 5 — Sustain and Optimize: TBD Pending Confirmation of funding

- Transition from remediation governance to steady-state asset and service governance.
- Conduct annual strategy, lifecycle, risk, workforce, and architecture reviews.
- Perform periodic recovery, continuity, failover, cybersecurity, and operational readiness exercises.
- Continuously improve alarms, analytics, predictive maintenance, and reliability.

6. Governance Structure

AIM Optimization and Stabilization cross-functional team

Provides direction, resolves cross-organizational issues, approves funding priorities, accepts risk and authorizes recommendation closure.

Program Management Office

Maintains the integrated master schedule, corrective action register, risk register, financial status, decision log, dependency map, and evidence repository.

Workstreams

1. AIM Strategy and Continuity
2. RTU and Communications Modernization
3. Configuration, Data, Alarm, and Performance Management
4. Vendor, Contract, and Workforce Continuity
5. Cybersecurity and Access Management
6. Enterprise Risk, Safety, and Physical Security

Independent Assurance

Internal Audit, Quality Assurance, Safety, Cybersecurity, or an independent technical assessor should validate controls and supporting evidence before closure submissions.

7. Performance Dashboard

Leadership reporting should include:

- Recommendations open, due, overdue, and ready for validation.
- High and critical risks by category.
- AIM availability and major outage trends.
- RTU availability, failure rate, and replacement progress.
- Fiber conversion progress and dark territory events.

- Alarm volume, nuisance-alarm percentage, and repeat alarms.
- RCA completion and corrective action closure.
- Backup and recovery test results.
- Configuration discrepancies and unauthorized changes.
- Vulnerability, POA&M, segmentation, and access-review status.
- Workforce backup coverage and training completion.
- Vendor performance, invoice exceptions, and cost recovery.
- Budget status, forecast, and modernization expenditures.

8. Funding and Resource Strategy

The program should establish a multiyear funding plan that separates:

- Immediate risk reduction and operational continuity.
- AIM sustainment and lifecycle support.
- RTU and communications modernization.
- Cybersecurity remediation.
- Data and analytics capability.
- Physical security upgrades.
- Workforce development and independent engineering support.
- AIM replacement or successor-platform investment.

Funding requests should be supported by risk reduction, operational impact, lifecycle cost, safety relevance, modernization dependency, and avoidance of recurring vendor or maintenance costs.

9. Communication and Reporting

- Monthly workstream status reports.
- Monthly centralized cross-functional team review.
- Quarterly executive and OIG-response reporting.
- Immediate escalation of safety-significant, operationally critical, or materially overdue issues.
- A controlled evidence repository containing approvals, assessments, procedures, test results, invoices, training records, risk decisions, and validation documentation.
- Consistent messaging to employees, vendors, operational stakeholders, and oversight organizations.

10. Expected Outcomes

Successful execution of this plan will:

- Preserve safe and uninterrupted rail operations.
- Establish an approved future state for AIM and supervisory control.
- Reduce reliance on obsolete assets, vendors, and key individuals.

- Improve RTU, communications, alarm, and system reliability.
- Strengthen configuration, data, cybersecurity, contract, and physical access controls.
- Improve management visibility through measurable KPIs and transparent reporting.
- Demonstrate sustainable corrective action rather than short-term audit remediation.

Report Fraud, Waste, or Abuse

Please Contact:

Email:	hotline@wmataoig.gov
Website:	wmataoig.gov/hotline-form/
Telephone:	1-888-234-2374
Facsimile:	1-800-867-0649
Address:	WMATA Office of Inspector General Hotline Program 500 L'Enfant Plaza SW, Suite 800 Washington, D.C. 20024